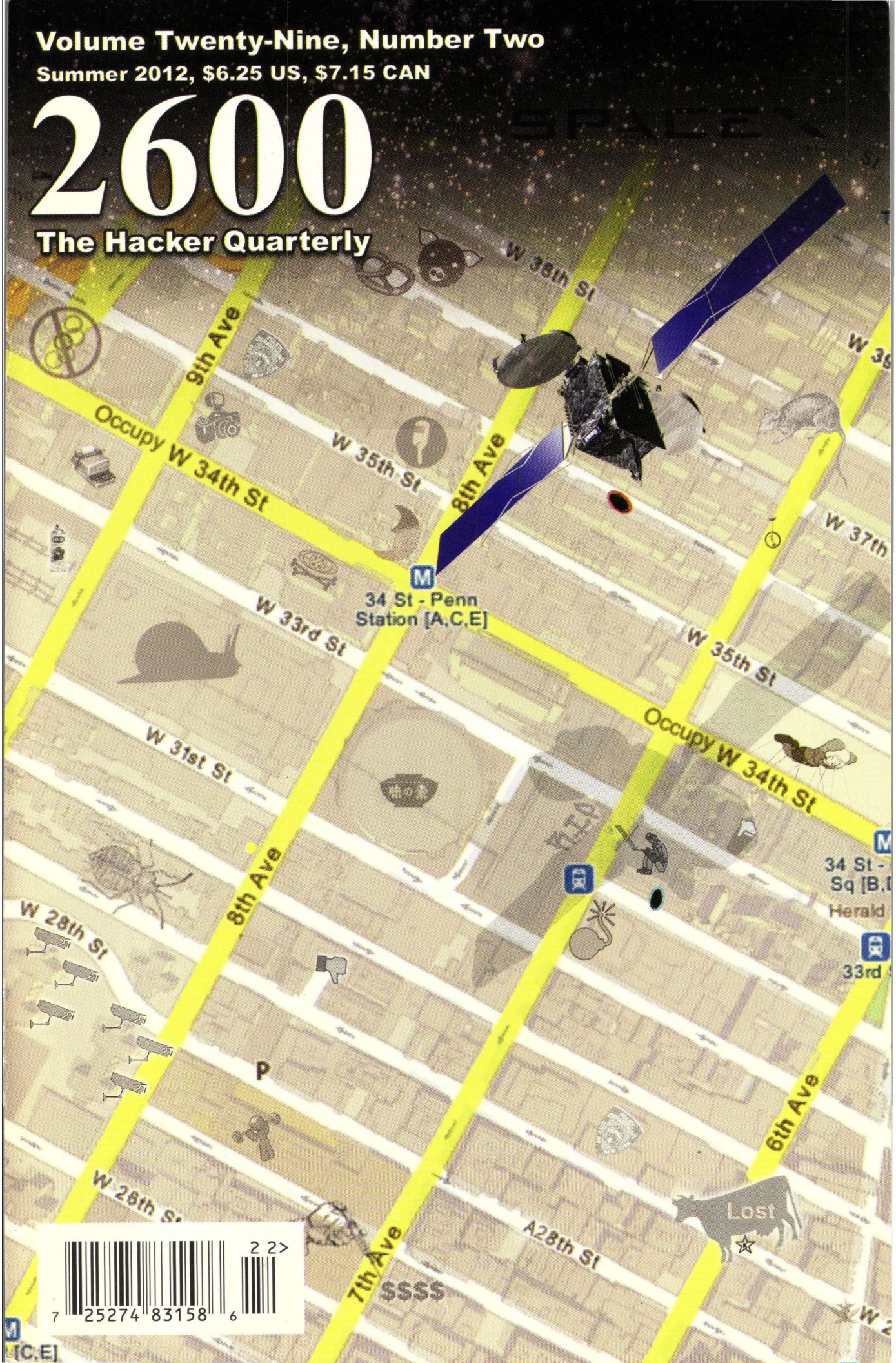
Volume Twenty-Nine, Number Two
Summer 2012, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



7 25274 83158 6 22>

Global Payphones

Russia. It is strictly forbidden to take any pictures in, on, or around airports in the Russian Federation. Even the payphone looks angry. This one was found in the Yakutsk airport.

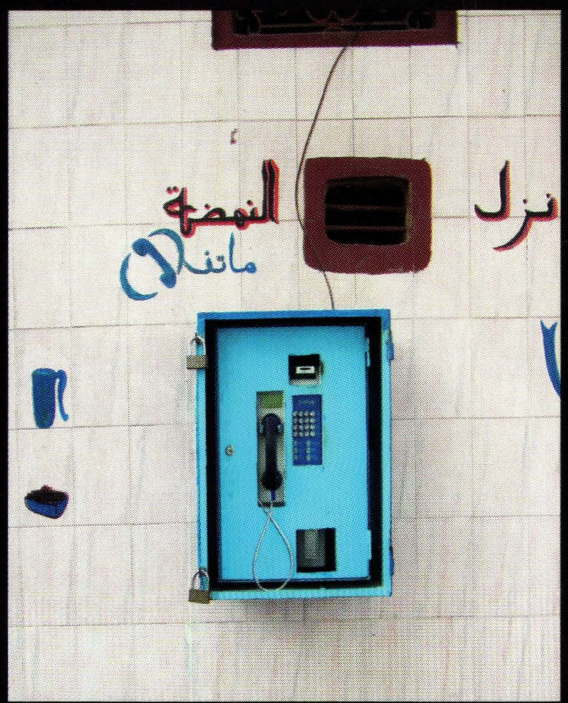
Photo by Robert

New Zealand. Found in the Post Office Square of Wellington, this phone does something weird: when you pick it up, you hear the sounds of a crowded French cafe instead of a dial tone. But you can still dial.

Photo by Breto

India. This "coin box telephone" was spotted in a forgotten corner of a New Delhi department store.

Photo by Jack Jordan



Morocco. Probably one of the most secure payphones around. Spotted in Tangier, this one only takes coins.

Photo by TProphet

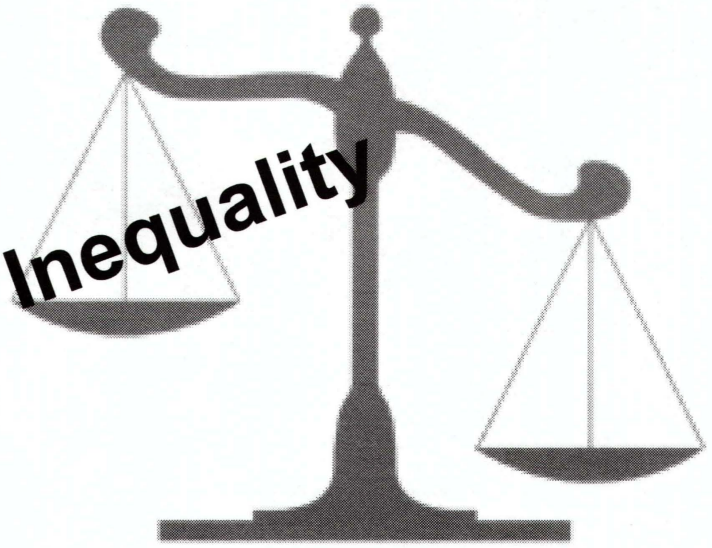
Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

BCNU

freedstock

Scales of Inequality	4
Bluetooth Hunter's Guide	6
Security by Obscurity = Insecurity	10
Building a Cat-5 Cable Tap	11
NGFW - Not Grandpa's Firewall	12
TELECOM INFORMER	13
A Counterpoint to "The Piracy Situation"	15
The Piracy Situation: The Devil's Advocate	16
Why is Piracy Still Allowed?	18
The New Age of the Mind	19
Building the Better Brute Force Algorithm	21
HACKER PERSPECTIVE	26
Firewall Your iPhone	29
Memoir of a Tech Writer: The Art of Leverage	32
LETTERS	34
Say It Ain't So Verizon	48
Hacking Climate Change With WeatherLink	49
Baofeng UV-3R: The Cheapest Dual-Band Ham Radio HT	51
TRANSMISSIONS	52
Metaphasic Denial of Service Attacks	54
Never Be ON TIME Again!	55
Fiction: Hacking the Naked Princess 1 & 2	57
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

Scales of Inequality



We've written in these pages many times to give examples of individual injustice, where someone is imprisoned or otherwise persecuted for little good reason. We now face something far more systemic, where such miscarriages become the rule rather than the exception, and where they're applied in a grossly disproportionate manner.

No case currently illustrates this better to our community than that of Richard O'Dwyer, a 24-year-old university student from Sheffield, England. Back in 2010, his website (tvshack.net) was taken down by the U.S. government, using one of those takedown banners we've become all too familiar with. The reason? O'Dwyer's site provided links to other sites that allegedly provided access to copyrighted material. *Links,* not the material itself. He was not accused of hosting any of this material himself and what he was doing isn't even considered a crime in England. Nevertheless, the site included the warning: *"TV Shack is a simple resource site. All content visible on this site is located at 3rd party websites. TV Shack is not responsible for any content linked to or referred from these pages."* Such disclaimers are quite common and, ironically enough, you can even find them on pages run by the U.S. government whenever there's a link to an outside page.

What we've just described is bad enough and indicative of the unequal and bullying power that the U.S. government wields in cyberspace. If only that was where it ended.

Not content to simply take a site off the net through their intimidation tactics and because the corporate powers in the United States want it to be known that they write the rules, the authorities have decided to go one step further. They are demanding that O'Dwyer be extradited to the United States to face trial and imprisonment! Perhaps even more astounding is that his own government in the United Kingdom has agreed to do just that.

Now, keep in mind that O'Dwyer didn't visit the United States and break this country's laws. (It's not even clear that this would be considered a crime here, anyway.) There is no serious contention that he committed a crime in the jurisdiction where he lived. The mere thought of a foreign country being able to simply pull someone out of their home and send them on a plane to a distant land to face their version of justice is something the vast majority of people would never consider to be a reality. And yet, here we are.

It should be noted that the treaty signed between the United States and the United Kingdom which allows this is basically a one-way treaty, meaning that United States citizens are protected from having the same thing happen to them. So, here, once again, we see the blatant inequality with which laws and justice are being applied. Imagine the outrage we would feel if *any* foreign country forced one of our citizens to face trial in their land for something that's not a crime here and which wasn't done on their soil. Why does our government feel that the rules should be any different for anybody else? And why don't we protest this sort of thing as vehemently as we would if it affected our own citizens?

The O'Dwyer case is far from an isolated one. But, as we said, this is one that those of us in the hacker community should be far more impacted by. Such a case shows that anyone

who accesses a U.S. based computer system without authorization, runs afoul of the Digital Millennium Copyright Act, pisses off powerful corporations, or is involved in any number of other potential violations, faces a one-way ticket to the States to answer charges. Even that scenario sounds rosier than it actually is. A foreign citizen who arrives in the United States to face trial isn't going to be allowed to simply walk around and go shopping until the proceedings get underway. They will be imprisoned from the moment they arrive, much like an accused "enemy combatant" would be.

In the States, we've managed to become used to the ill-advised logic that justifies imprisoning foreigners in a U.S. base without trial because they're suspected of fighting against our troops in their own country. Imagining the same scenario in reverse would be practically unthinkable to us. But if we don't, we run the clear risk of elevating ourselves above the rest of the world and living by a completely different set of rules and laws. This sort of thing has happened throughout history, whether through invading forces or divisions of class. It never ends well for those who see privilege as their right. And it *always* ends at some point.

Selling the idea of bringing supposedly dangerous terrorist types to justice in this manner may not have been too much of a challenge to a terrified public. But when it starts to be applied to everyone else, as it inevitably tends to be, the damage to society and international relations can be irreparable.

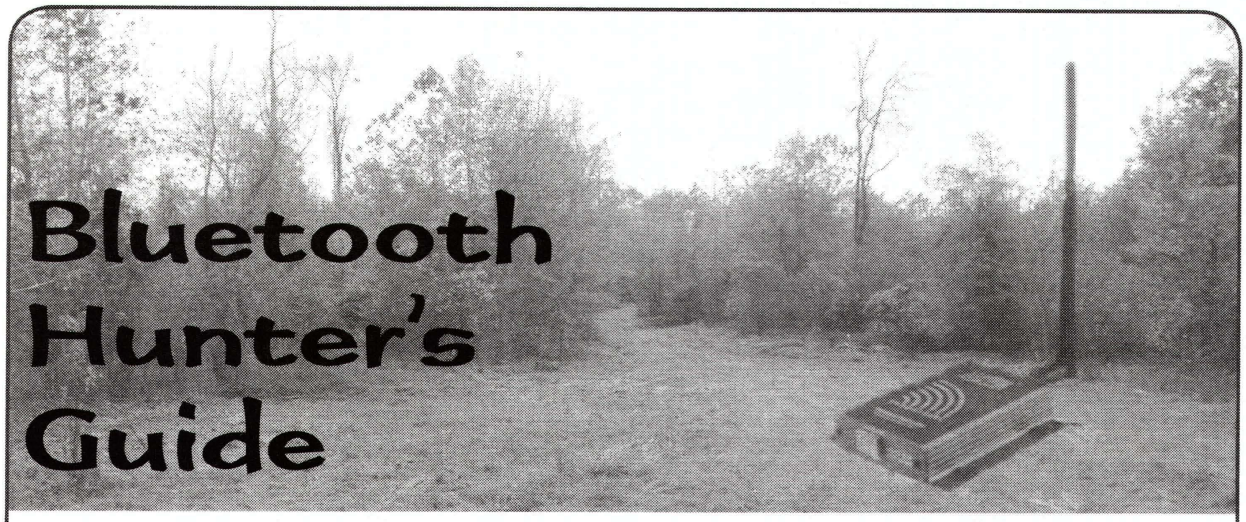
With regard to the specifics of the case we're citing, the law in question is known as The Extradition Act 2003, passed by the Parliament of the United Kingdom, and which went into effect in January 2004. Amazingly, the Act doesn't even require evidence to be presented to obtain an extradition. Rather, "reasonable suspicion" is all that is needed.

Richard O'Dwyer is far from the only person to be victimized by this flawed treaty. Many in the hacker world will have heard of the case of Gary McKinnon, accused of hacking into military computers in the United States in 2001 and 2002. His claim was that he was looking for evidence of UFO cover-ups and free energy suppression. The U.S. government claims he deleted logs and shut down a network of 2000 computers for 24 hours. McKinnon himself admits to leaving an ominous message saying "I will continue to disrupt at the highest levels." Even though the extradition act was passed after these alleged offenses, they are being applied retroactively. Regardless of how one feels about the motivations of McKinnon, surely the only way to handle it can't be to send him to a foreign country where he faces 70 years in prison. If what he did was, in fact, a crime, is the United Kingdom unable to handle prosecuting it themselves? Or would they perhaps not handle it in the same exaggerated manner that the U.S. is known for, thereby not sending the desired message of fear and subservience?

There are a number of other cases involving extradition to the United States that are in the news. Some involve people who worked on websites tied to groups defined by the U.S. as terrorist in nature. Some were involved in financial offenses, such as the NatWest Three, accused of crimes "committed by British citizens living in Britain against a British company based in London." The British government didn't prosecute due to lack of evidence, but that didn't stop the Americans from having them extradited and sentencing them to 37 months in prison, plus time spent waiting for trial.

It's well known that the federal government would love to have Wikileaks founder Julian Assange in their clutches, for no other reason than the embarrassment that was caused by the infamous leaks, and to send a message to anyone who dares to think of whistleblowing. Treaties like this one will make such a wish easily obtainable and anyone who annoys our government will be fair game, regardless of whether or not they actually committed a crime.

As we go to press, reports are being circulated that the governments of the United States and Israel were, unsurprisingly, behind development and release of the Stuxnet worm that sabotaged the computer systems at Iran's nuclear facilities. In the eyes of the civilized world, this sort of attack is far more serious and easily definable as a crime than any of the above examples. Yet, prosecution and extradition of those responsible will almost certainly never occur. In such a world of inequality and malformed justice, how are people here and abroad seriously expected to ever believe that the system is fair and that it actually serves their interests?



Bluetooth Hunter's Guide

by MS3FGX
MS3FGX@gmail.com

Since the publication of my article "Bluetooth Hacking Primer" in 27:1, I have received quite a few questions from readers who were curious about the practicality of Bluetooth attacks in general. One of the most common questions is, understandably, how many vulnerable Bluetooth devices are out there in the first place?

That's not quite as straightforward a question as it might seem. It's important to realize that not all discoverable devices are vulnerable to attack, nor are all vulnerable devices discoverable (more on that later). Discoverable devices are simply that, devices which we can easily detect. If nothing else, scanning for discoverable devices is useful for determining the density of Bluetooth devices in a given area. If an attacker can establish where the most users of Bluetooth devices are, they will know where to focus their efforts.

A lot of modern devices aren't discoverable at all unless specifically enabled and, even then, they usually only stay discoverable for a few minutes. While it's great that newer hardware and mobile operating systems are taking a more pragmatic approach to Bluetooth security, it doesn't do anything for the millions and millions of older devices already out in the wild. Of course, not all manufacturers are so enlightened either, so there are still some new devices that are shipping with questionable default policies. The end result is that there are still many Bluetooth devices happily announcing their presence to anyone who cares to listen.

This particular article will focus on the search for, and identification of, Bluetooth devices on a large scale. We'll start by looking at the best hardware for long-range omnidirectional detection, and then talk about some different software options and techniques available. I'll also be discussing some of the data I have personally collected to give you an idea of what you should expect in terms of number of results and the identifiable information therein.

Hardware Setup

My main workhorse is the AIRcable Host XR, an extremely powerful USB Bluetooth device that is primarily designed for proximity marketing. It has a 200 mW radio (twice the power of a normal Class 1 device) and a standard RP-SMA antenna connector, which makes it perfect for long range applications. With the Host XR connected to a directional parabolic antenna, I have been able to establish a connection with a moving cell phone at over 350 meters - careful aiming and a more docile target would push that number even higher. As an added bonus, the Host XR uses the very well supported Cambridge Silicon Radio chipset that I mentioned in the previous article, so it will work out of the box on any modern OS as well as support the extended feature sets used in some software.

If there is any downside to the Host XR, it's cost; at $130 USD you need to be pretty into this sort of thing to make the purchase worth it. Luckily, older versions of the Host XR sell on eBay for around $60, which is considerably more reasonable for the experimenter. The older versions of the Host XR (XR1 and XR2) are identical to each other. The XR2 simply has a nicer case and a bit more mass-market friendly blister packaging (the XR1 I purchased from AIRcable literally came in a Ziplock Freezer bag). The current model, XR3, is claimed to be even more powerful than the XR1/2, but I haven't been able to personally verify this.

The parabolic antenna is great for range, but just a tad bit suspicious when sitting in the food court at the mall. For general scanning, I go with a 3 dBi "rubber ducky" antenna which makes the whole package easy to conceal in a standard laptop case. If I'm going to be scanning from a location where the hardware won't be visible, I bump the antenna up to a 9 dBi (the 9 dBi is about

16 inches long, and tends to get some glances), which pushes the range up to nearly 300 meters. Even with a tiny 3 dBi omni, the Host XR can pick up devices at around 250 meters, which is still twice the "maximum" range for Bluetooth.

That being said, there is no technical reason you couldn't use your machine's internal Bluetooth hardware or a cheap USB adapter. Any Bluetooth device is capable of scanning; the issue is one of power. Using low-power hardware is fine for testing and getting a hang of the software, but with a range of 10 meters (or less), you aren't likely to get many results outside of the devices sitting on your own desk.

Discoverable Device Scanning

Discovery scanning is the most common and effective way of finding information on Bluetooth devices. Fundamentally, it's based on the same process that two Bluetooth devices use when attempting to make a legitimate connection, such as pairing a phone to a headset. Before Bluetooth devices can connect to each other, at least one of them has to publicly announce their presence. Discovery scanning exploits that fact to collect information anonymously.

One of the interesting things about Bluetooth discovery scanning versus something like Wi-Fi scanning is that there are three distinct steps required to collect all of the pertinent data for each device. The first step is to command the hardware to scan all available channels for discoverable devices and return their MAC addresses. Once the list of MAC addresses is gathered, each device will be queried individually to determine the device's human friendly name. With the device's MAC and name recorded, the system can then use Service Discovery Protocol to find out what high-level services the target device offers.

It's worth noting that only the first step, getting the MAC address, is technically required to establish a connection with the remote device. Since each subsequent step takes a few seconds to complete, it is often desirable to forgo the third and even second steps for the sake of time and accuracy. This is especially true when dealing with moving targets or when working with short range hardware; if there are ten devices reported during the initial scan, and it takes one or two seconds to complete the second and third steps, the time required to gather all of the information for each device quickly compounds to the point that a particular device may have moved out of range since its initial discovery.

The following are tools for Bluetooth discovery scanning which are worthy of your attention if you plan on doing experimentation of your own. There are a number of other tools available, but they tend to be only lightly featured or in some cases abandoned.

btscanner

Arguably the best known Bluetooth scanner, btscanner [1] is even included in the package repositories of many Linux distributions. btscanner is very easy to use and collects an incredible amount of information without needing to pair with the target devices. The information is presented in a ncurses-based user interface that was clearly inspired by Kismet, something unique among Bluetooth scanners.

If there is any downside to btscanner, it's that it hasn't seen an update since 2004 and its age is starting to show. There are a number of rather annoying UI bugs, and the more advanced features present in the new breed of scanners is notably absent. An option to compile and run btscanner without ncurses is also sorely missed, and could be a serious problem depending on your requirements.

Stalled development aside, this legacy tool is still useful for the occasional quick scan and the fact that many distributions include it certainly helps to keep it popular.

SpoofTooph

SpoofTooph [2] is not a Bluetooth scanner in the strictest sense. While scanning for Bluetooth devices is one of its core features (and something it does very well), it's primarily designed to spoof or clone Bluetooth devices.

SpoofTooph first scans the area to locate devices which are in discoverable mode, then allows you to select one of them to spoof. Spoofing a Bluetooth device can be used for a number of purposes, such as attempting to circumvent applications which use a Bluetooth device (such as a mobile phone) as a security token. You can also load your Bluetooth device up with completely fictitious information, which could be used to make legitimate Bluetooth communication more difficult.

Its more advanced functions aside, SpoofTooph is an excellent scanner as it presents results in a very intuitive and easy to read format in the terminal with minimal configuration or interaction from the user. All discovered devices can be logged to a plain text file, and SpoofTooph even includes a log reader mode where it can reload a previous scan's results for later review and cloning.

Harald Scan

Harald Scan [3] is a modern Bluetooth scanner written in Python, perhaps best known for its ability to determine device manufacturer via the largest known Bluetooth MAC address vendor list.

Harald Scan offers a number of very nice features not found in other scanners, such as the ability to update its MAC vendor list via the Internet, optional service scanning, and metrics showing how many devices have been discovered in a given time frame. Its user interface is very simplistic, but gets the point across. Devices are logged in an easily parsed XML format which is ideal for exporting the data into other applications or formats.

Active development, cross-platform support, and unique features make Harald Scan an excellent tool for general Bluetooth scanning.

Bluelog

All right, full disclosure time. Bluelog [4] has been my personal project for over a year now. I wrote Bluelog because all of the Bluetooth scanners I found seemed to be designed around the same basic idea: that you wanted to stare at a display of all the devices being discovered in real time, and maybe save a log at the end of the scan. But what I really wanted to do was scan over a long period of time and log directly to file without having to monitor the software or interact with it in any way.

Because of my rather specific goals, Bluelog is unique among Bluetooth scanners for a number of reasons. The major difference between Bluelog and other scanners is that it has no user interface to speak of, just some boilerplate and status information as it starts up. Though enabling verbose mode will let you see devices as they are discovered, Bluelog's primary method of output is real-time logging to file. By saving results in real-time, you can kill Bluelog at any time and be sure all of your data has been recorded. Bluelog is also (to my knowledge) the only Bluetooth scanner to feature a daemon mode, where it can drop into the background and log discovered devices to file indefinitely.

Probably its most unique feature is Bluelog Live, a special mode where discovered devices are displayed via a constantly updating web page, with each device's pertinent information laid out in plain English. Inspired by the infamous "Wall of Sheep" display, the goal of Bluelog Live is to raise public awareness of the implications of discoverable Bluetooth devices. Running at a hacker convention or other public gathering, Bluelog Live should provide viewers with an eye opening look at the amount of identifying information they are broadcasting.

Non-Discoverable Device Scanning

Scanning devices in discoverable mode is easy enough, but what if you wanted to find devices that weren't actively transmitting their presence? While far from ideal, it is possible to scan for non-discoverable Bluetooth devices by exploiting a core concept in the Bluetooth protocol: even if a device is not in discoverable mode, it still has to answer to requests for information so that it can communicate with legitimate peers.

Instead of listening for broadcasting devices, non-discoverable scanning queries individual devices by MAC address for their configuration information (such as the "friendly" device name). The target device is obligated to respond to such requests, regardless of discovery settings and without so much as a prompt on the target device's screen. The problem is, this only works if we already know the MAC address of the target device, which at this point we don't. Since we don't know the MAC address of the target, and it isn't broadcasting, the only remaining way to find the MAC is by brute-forcing it.

To brute-force a Bluetooth MAC, the software will sequentially step through a predefined range of MAC addresses, pausing on each one to perform a device inquiry. When and if the scanner receives a response, it can log that MAC and associated information to file. The process can be sped up considerably by using multiple Bluetooth adapters to parallelize the operation, and the MAC range can be narrowed a bit if you know the manufacturer's OUI. Still, given the sheer number of possible MAC addresses and the fact that it takes a few seconds for the device inquiry (whether there is a response or not) to complete, brute force scanning is a very daunting task.

Realistically, scanning for non-discoverable devices is only practical if you are targeting a single device whose manufacturer and make you have already established visually. Even with enough information to narrow your MAC range and multiple adapters working the queue, it's going to take a very long time to complete a single pass. The scope of this method is exceptionally limiting, but if you are targeting something like a Bluetooth enabled desk telephone in an office building, it's possible.

If you want to experiment with brute force Bluetooth scanning, the best tool available is the one that introduced the concept in 2003, RedFang [5]. While it's rather simplistic and hasn't seen development in quite some time, it's still the most reliable tool for this type of device scanning.

Real World Results

While doing some research on past Bluetooth security talks and demonstrations, I found a very interesting white paper put out in May of 2006 by F-Secure and Secure Network entitled "Going Around with Bluetooth in Full Safety" [6]. The paper details how the group constructed a mobile

Bluetooth scanning rig disguised as a pull-along piece of luggage and wandered around Milan with it during Infosecurity 2006. After seven days of scanning at various high-traffic areas, the team recorded 1,405 devices, which at the time made something of a stir and grabbed a few headlines in various tech publications.

The paper goes on to say that their scanning rig never attempted to connect to any of the discovered devices, and that simply being discoverable does not necessarily mean the device is exploitable. The exercise was merely to gauge the proliferation of Bluetooth devices, specifically, those left in the ill-advised discoverable mode. The paper concludes that the number of discoverable devices in the field is already high and that as smartphones become the norm in the near future, this number is only going to go up.

Reading this article five years after its publication, I couldn't help but wonder how the situation may have changed. The authors correctly predicted the era of the smartphone, but have manufacturers wised up about Bluetooth security?

With this in mind, I set up my own similar experiment which I deemed "Operation Street Sweep" [7]. In my version, I installed Bluelog on an OpenWRT router and connected it to one of my AIRcable Host XR Bluetooth adapters. I then placed the rig within a hundred meters or so of a fairly busy intersection and shopping plaza. After only five days of scanning, my setup had recorded a staggering 2,596 unique Bluetooth devices.

I was completely blown away, first by how many devices I was able to record, but also how much information I could glean from them. Taking a close look at the records showed there were all kinds of identifying information hidden within the MAC addresses and device names. For example, Garmin in-car GPS units have their serial numbers in their device names, and the iPhone conveniently broadcasts the owner's full name. I also saw a number of devices whose owners had made the name their online handle. A quick search on Google, and I was well on my way to identifying the individual.

What's more, if we allow devices to be logged multiple times over a long duration scan, the timestamps can be compared each day and a timetable could be constructed for each individual MAC. This rough schedule, paired with the unique identifying information for a specific device, would allow an attacker to get a good idea as to where the target is at a particular time. In its most basic form, this technique could be used to determine when a target is away from their home.

Conclusion

Experiments like this, performed with open source software and readily available consumer hardware, show just how much information is being beamed out for anyone who cares to listen. With thousands of devices eagerly announcing their presence and identifying their owners, even a very low success rate on attacks could be a real threat. Even if we assume that only one percent of discoverable Bluetooth devices are vulnerable to attack (through either social engineering or exploitable implementations), there are enough targets that it's still feasible to hit a few devices a day successfully.

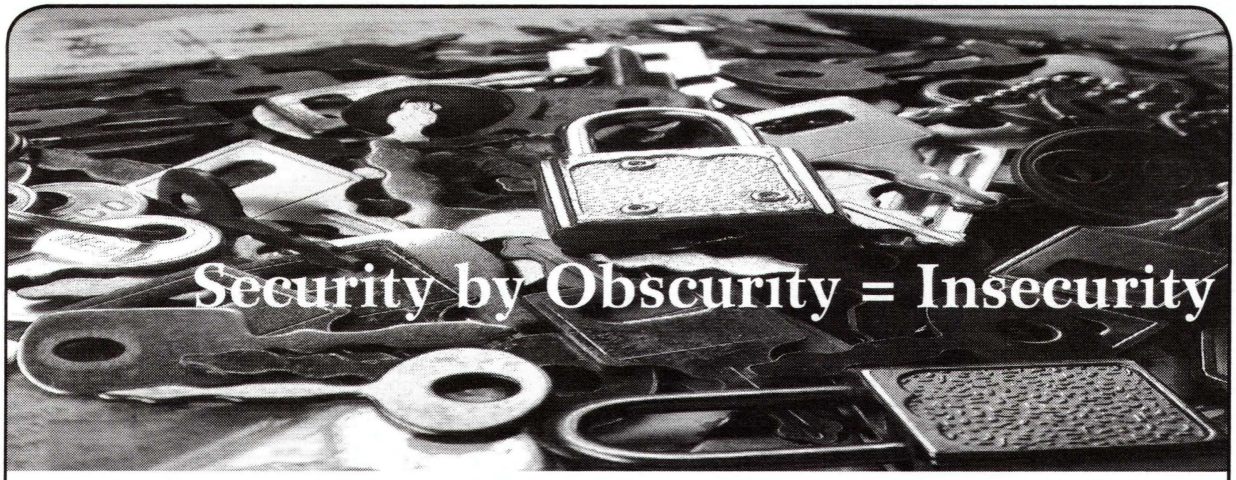
Hopefully, this article has given you enough information on the ideal hardware and available software to launch your own research. Keep in mind that the results I obtained in my experiment were not due to some magic combination of hardware, software, and location. I believe these results to be representative of average Bluetooth device density, and should be easily repeatable. I've also performed numerous scans at public locations such as malls, movie theaters, and restaurants. I've found that malls are very good places to conduct scans, especially at peak shopping times like the holidays. In a well populated mall, I've had no problem picking up upwards of 100 unique devices per hour, even with a standard Bluetooth adapter.

In fact, I'm willing to bet that in more densely populated areas, my results would be put to shame. I'd be very interested in hearing from anyone who conducts similar experiments using the methods and software mentioned in this article. I've been thinking about a distributed effort to catalog and map Bluetooth devices and their relative density (like WiGLE [8] for Bluetooth), and would love to compare notes.

Good hunting!

References

1. http://www.pentest.co.uk/src/➥btscanner-2.1.tar.bz2
2. http://www.hackfromacave.com/➥projects/spooftooph.html
3. http://code.google.com/p/➥haraldscan/
4. http://www.digifail.com/software/➥bluelog.shtml
5. http://www.securiteam.com/➥tools/5JP0I1FAAE.html
6. http://www.securenetwork.it/➥ricerca/whitepaper/download/➥bluebag_brochure.pdf
7. http://www.digifail.com/research/➥streetsweep.shtml
8. http://www.wigle.net/



Security by Obscurity = Insecurity

by DocSlow

The rather expensive education of protecting your personal belongings from theft offered up by many so-called security "experts" usually involves obfuscating the simplicity with which most barriers can be bypassed. This is simply a part of the flawed concept of "security by obscurity" that many self-proclaimed security authorities pass on to everyman as their intimate brand of super-secret technical wizardry. These security experts want us to believe that they can, for a fee, mentor us on how to secure our most treasured belongings. More often than not, their instruction is completely invalid.

Last year, at Defcon, there was an entire ballroom reserved for nothing but lock picking. Hackers have always had a romantic fascination with picking locks (myself included), and this ballroom was packed with those who were teaching techniques, some of them selling wares, and there were a host of avid students of the sport.

Let's just focus for a minute on your transportation. I'm sure you've all seen the movies where there are elaborate collections of "high-tech" tools used to start a car (especially those with a steering console ignition) minus a key. Usually, these absurd methods either involve large vise-like tools (e.g., slide hammer puller) that remove the lock from the console (and expose an abysmal myriad of color-coded wires), or the use of brand-specific bypass keys, and many yet still show the silliness of pulling a few wires from underneath the dashboard to simply "hotwire" the ignition. Most of these Hollywood techniques irreparably damage the vehicle in some way, and all of them offer nothing in the form of car-jacking reality. Real car thieves are having a good laugh.

A good locksmith (one that knows the true intricacies of locking mechanisms) can open your car and start it in seconds, without the use of any high-tech gear. No need for Slim Jims, pick guns, or Lever Wedges (expensive lock picking tools marketed to the programming equivalent of script kiddies). The job can be done with nothing more than a couple of simple rake picks. And the beauty of a steering console ignition is that you don't need any sophisticated external leverage device to turn the lock - it's built in to most console ignition locks.

While I've heard that the use of two simple jagged rake picks can do the job in short order, one might also use a snake rake pick and a double ball pick. But simple rake picks work just fine, as they do on almost all locks.

To test this theory (one that I acquired from real experts), I performed a quick trial run on several subjects that included all manner of console ignition switches, and all turned out to be easy "pickings."

My first test case, a 1995 Jeep Grand Cherokee, proved to be a reference standard for all other experiments. The first attempt at entering the vehicle and successfully starting it took a little under 30 seconds. Most others took a similar amount of time.

And, remember, the beauty of 4-inch slender picking tools is that if the cops show up in under the 30 seconds it takes to drive off with your cache, you can quickly and easily hide them in your shoe (or wherever your imagination takes you), and claim that all cars look alike these days.

Oh yeah, and getting into your house is even easier.

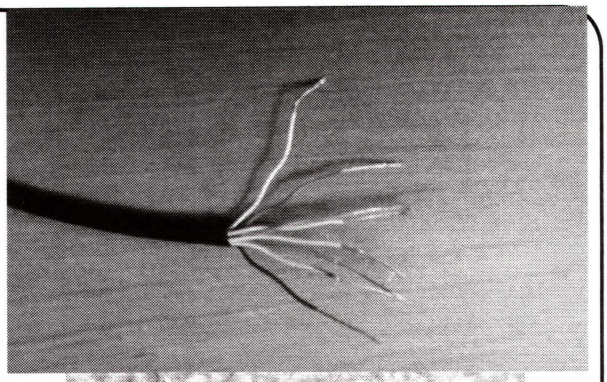
No, I'm not providing you with exact details on how to do this, but, we're just speaking hypothetically here (yes, that's a disclaimer).

To quickly conclude... this is why some governments hire hackers. Hackers don't bullshit you about your security. They show you how easy it is to break in and steal your shit (after the "security experts" have "consulted" you that your security is now OK - subsequently implementing a whole host of useless measures), and hackers prove that their possession of real security knowledge far surpasses that of the "security expert."

Obscure that.

BUILDING A CAT-5 CABLE TAP

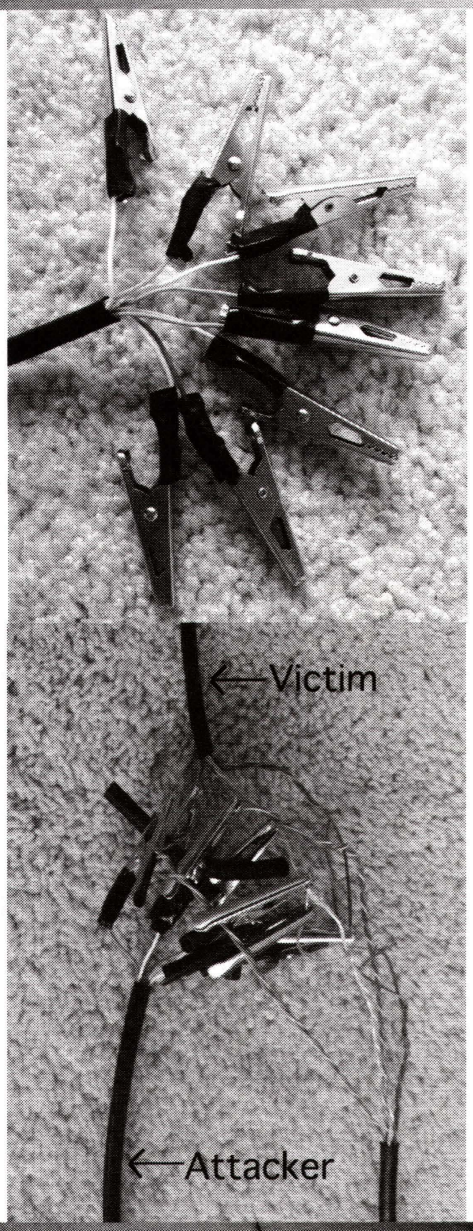
by Ashes



This article is a tutorial on how to build a special Cat-5 cable to physically tap into an existing Cat-5 cable. The idea came to me on a deployment in Iraq when our Tactical Operations Center (TOC) had numerous Cat-5 cables that were exposed (the TOC was manned 24x7). I thought how easy it would be in a corporate environment to connect a physical tap to one of these wires, most commonly found in drop ceilings.

The first step to making this tap cable is to cut one of the ends. If creating from a reel of cable, leave one of the ends exposed and terminate the other end with an RJ45 connector. The next step is to strip the outer coating and each individual wire, exposing the metal wire.

Next, you need to solder the bare metal wires to alligator clips. In the image below, I soldered and taped the ends for a stronger hold.

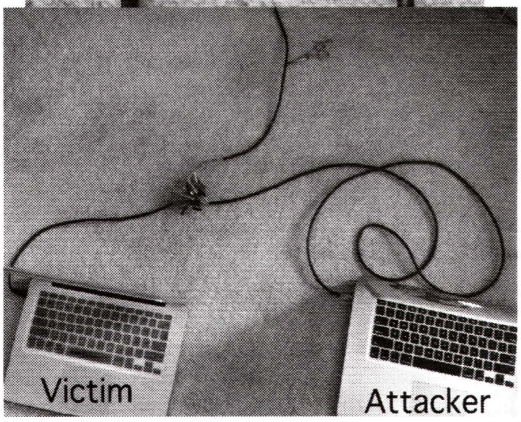


Now that your cable is built, it is ready to attack (or test, depending on your hat color). To begin the attack, you need to strip the victim's Cat-5 cable (all individual wires) down to the metal without cutting it. Tricky - it takes patience and finesse. After the metal of all the wires has been exposed, you can connect the attacking cable's alligator clips to the victim's exposed metal wires.

Important: When connecting the alligator clips, you must match the colors from the attacker's cable to the colors of the victim's cable. For example, blue-white on attacker cable needs to attach to blue-white on victim cable, etc.

Make sure that the alligator clips do not touch. In the above picture I used parts of the outer shell of the victim's Cat-5 cable to keep the clips separated. If the alligator clips touch, the connection will drop.

Once your attacking machine is connected to the Cat-5 tap cable, fire up the packet sniffer, go to promiscuous mode, and sniff away!



by Daniel Ayoub
daniel@ayoub.it

When you think 25 years are enough to understand a technology, think again. Firewalls have been around for nearly a quarter century. Still, some folks don't fully understand the technology, much less how it has changed and where it stands today.

As you would expect, the term "firewall" is a reference to the safety barrier installed in structures to stop blazes from spreading throughout the building. In the late 1980s, researchers developed a packet filtering system which could be used to inspect traffic as it crossed the network; "good" traffic was allowed in and "bad" traffic was dropped by the filtering system. Good traffic was defined based upon specific rules set up by the system administrator such as protocol, port, and MAC/IP addresses. If a packet came through the system that didn't match the predetermined filtering rules, it would be deemed "bad" and got blocked. These first generation firewalls operated at layer 2 and layer 3 of the OSI model. The term "firewall" was adopted to describe the technology since the new packet filtering system provided a type of virtual barrier for traffic entering the network.

The second generation firewalls from the early 1990s contained the same packet filtering technologies of their predecessors, but also incorporated the concept of "stateful" packet inspection (SPI). Through this feature, the firewall builds a table in memory to track connection streams. As new streams (sessions) are generated from the local area network (LAN) and headed (out) for the wide area network (WAN), the firewall created entries in its "state table." When traffic was sent back (in) from the WAN to the LAN, the firewall looked in its memory table for the matching outgoing session. If it found a match, the traffic was permitted and passed along to its destination. If no matching entry was found, the traffic was dropped and stopped from entering the LAN. Second generation firewalls still operated at layers 2, 3, and 4 of the OSI model.

Today, features like packet filtering and stateful packet inspection have been commoditized to the point that they're incorporated into cheap off-the-shelf consumer grade integrated router/switch combination devices. Stateful packet inspection and packet filtering are still present but as processing power grew, so did the capabilities of firewalls. Today's third generation firewalls are more of a smorgasbord of technologies rolled into one than earlier generations. Their features heavily rely on the concept of deep packet inspection (DPI). With DPI, the firewall inspects the contents of each packet that it passes. This provides the firewall with an entirely new level of intelligence and opens the door to a whole slew of possibilities.

Thanks to deep packet inspection, features like intrusion prevention, malware detection, gateway anti-virus, traffic analytics, and application control are all possible. Modern firewalls also incorporate technologies like IPsec VPN, SSL VPN, and SSL decryption right out of the same box.

Today's "next-generation firewalls" (NGFW) inspect the payload of packets and match signatures for nefarious activities like known vulnerability, exploit attacks and viruses, as well as malware on the fly. Deep packet inspection also means that administrators can create very granular permit/deny rules for controlling specific applications and websites (example: Yahoo instant messenger - chat is allowed but file transfers through YIM are not). Since the contents of packets are inspected, exporting all sorts of statistical information is also possible. This means admins and management can now easily mine the traffic analytics to perform capacity planning, troubleshoot problems, or monitor what sites individual employees are viewing throughout the day.

Where things will go next is anyone's guess, but one thing's for sure: these are definitely not grandpa's firewall.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! My gleaming new facility is finally online, busily routing all manner of traffic throughout Asia at volumes I've never seen before. The number of Internet users in China is roughly double the population of the United States, and with a daily population in Beijing at times exceeding 40 million (in between residents and visitors), demand for bandwidth greatly exceeds supply. Suffice it to say that Internet users here eat STM-64s for breakfast, and this is before you even begin to factor voice traffic. I have never seen anything like this in my life, but I could say that about hundreds of things in China. This is one truly amazing place.

Summer is one of my favorite times of the year in Beijing, and this is likely to be my last summer here as my time in China draws to a close. I live in the old city of Beijing, an area of temples and traditional courtyard homes. Many things here were built before Columbus discovered America. Hot summer evenings are great for enjoying sticks of roasted lamb *chuan'r,* drinking big bottles of Yanjing *pi jiu,* and watching the world go by. Payphones are still the primary method of communication for many of the elderly residents of this *hutong* neighborhood, and cheap GSM mobile phones are used by the many workers here. Old men ride tricycles stacked with cardboard for recycling, chattering loudly on their *shou ji* while weaving in and out of traffic. All of these scenes look like they belong in a movie, but for the last two years, they've been my daily life. What's next? I'm really not sure. I left my comfortable union job in the U.S., and don't have a new job lined up yet when this one concludes at the end of this year, so I leapt at the opportunity to book a trip on Worldtoor to Antarctica. It's a once-in-a-lifetime chance to see the most remote place on earth, but I'll still have job responsibilities up until the day I leave. Going "off the grid" is possible for a few hours, but not for a few weeks - and penguins don't have cell phones. The solution? Iridium, a global constellation of 66 low earth orbit satellites. The network offers connectivity between virtually any two points on the globe, but at the turn of the century it was nearly taken off the grid.

Iridium was the brainchild of globetrotting Motorola executives who saw an opportunity amid the frustrating and fragmented landscape of cellular and satellite providers of the early-to-mid 1990s. At the time, global roaming was generally not possible, and even domestic roaming was complicated (sometimes requiring pre-registration and three dollars a day plus 99 cent per minute fees). Satellite phones from Inmarsat weren't a good solution either. They literally came in a briefcase with a pizza box sized antenna and a full-size telephone handset reminiscent of bag phones. Airtime cost $10 per minute. Motorola researchers developed a handheld satellite phone that was small enough to wear on a belt clip, and then designed a cellular network in the sky to go with it. Six billion dollars (3.5 billion of which came from Motorola) and a whole lot of Chinese rockets later, and Iridium was born. The first call was placed by Vice President Al Gore on August 13, 1998.

And then, just nine months later, Iridium was bankrupt. Between the early and late 1990s, GSM rolled out in major U.S. markets (with VoiceStream and Omnipoint), tri-band GSM handsets capable of global roaming became available, and international roaming rates averaged $1.50 per minute. Meanwhile, the mass market that Iridium anticipated never materialized. For starters, the $2,000 Iridium handsets were bulky and already dated at launch time. They also didn't work indoors, in cars, in tunnels, or even outdoors in areas where tall buildings or trees or mountains or virtually anything else blocked an unobstructed view of the sky. It also didn't help that airtime cost seven dollars per minute, and that the sales staff was generally viewed as unhelpful and unresponsive. At bankruptcy, Iridium had only 15,000 customers with a total of 55,000 handsets.

Its shareholders furious at the continued bleeding of cash, Motorola sought to divest itself of Iridium as quickly as possible. Unfortunately, it was left holding the bag as the operator of the Iridium network, having given earnest guarantees to various agencies of the U.S. government that the satellites would be decommissioned in an orderly manner if service was discontinued. Barely a year after launch, Motorola began making plans to de-orbit the entire constellation, an endeavor that was estimated to cost between $30 and $50 million, and which NASA estimated carried a 1-in-279 chance of killing someone due to falling debris.

Numerous potential suitors bid in bankruptcy court, but none had either a credible plan to operate the business or to indemnify Motorola from responsibility to decommission the satellites (which Motorola reasonably insisted on being a condition of sale). After numerous failed bids, Iridium handsets lost connectivity to the public switched telephone network (PSTN) on August 25th 2000, when the gateways were decommissioned and it really looked like it was over. With only a few days until the stratosphere would begin raining satellites, a consortium called Iridium Satellite led by former Pan Am executive Dan Colussy entered a credible bid in bankruptcy court. In effect, it was a three-way deal between Iridium Satellite, Boeing, and the U.S. government. Iridium Satellite would provide a seasoned management team and $25 million in investment. Boeing would take over operating the satellite constellation from Motorola. And finally, Uncle Sam was standing with his checkbook open, ready to sign a sweetheart contract worth three million dollars per month, buying unlimited minutes on up to 20,000 handsets for two years. The bankruptcy judge agreed, original investors lost their shirts, and Iridium quickly restored service.

Under the Colussy regime, customers were no longer globetrotting executives needing to be reached on the beach. Presumably, Pan Am had taught him about the importance of connectivity in remote parts of the world, and Iridium began focusing on customers who needed coverage that simply wasn't available anywhere else. What's more, rates dropped by substantial margins, to as low as $1 per minute. Iridium's new customers were in places like the South Pole, where Iridium is the only working service, or mountaineers climbing in the Himalayas, or oceanographic telemetry. The technology allows for Iridium to be used at any point on the globe, but some countries (such as North Korea) have requested that Iridium block the service - and Iridium honors such requests.

Call and service quality on Iridium is generally poor. Voice channels run at a maximum data rate of 3.3Kbps (by comparison, a standard GSM voice channel is 64Kbps), using the Advanced Multi-Band Excitation codec. Although the Iridium system technically supports handoffs, dropped calls are common - the ideal usage scenario is in a completely flat location with no obstructions on the horizon above 15 degrees. Anecdotally, if these conditions aren't met, the call is likely to drop (making Iridium best suitable for occasional short duration calls).

Data service is available at 2400bps. You can terminate to either a dial-up modem or to the Internet via the Iridium gateway. While Iridium claims "up to 10Kbps Internet," this claim is based on V.42bis compression. You're likely to see compression on text or HTML, but not on compressed data such as image files. At the South Pole, Amundsen-Scott Station has 12 Iridium handsets operating in bonded dial-up, giving the station a theoretical maximum 28,800bps of bandwidth.

Handset development is slow. The first handsets were manufactured by Kyocera, but only Motorola makes current handsets. The models that are now in production are the 9555 and 9575. These are simple feature phones with no smartphone features and with no third party applications. Either handset can be connected to a PC with a USB cable. Alternatively, an "AxxessPoint" mobile hotspot device is available.

All billing is in terms of airtime minutes, which are generally prepaid. The price is variable depending on your subscription package and the number of minutes you buy. Some airtime packages are geographically limited (and billed at a lower rate) while airtime usable worldwide is more expensive. Incoming SMS is free and there is a web interface for sending SMS to an Iridium phone. Outgoing SMS is billed at .33 minutes per message. Iridium accounts have a telephone number in the +8816 country code (generally in the 31X-XXXXX range), and can also be assigned a number in the +1 480 NXX. Incoming calls to the +8816 number are free, while incoming calls to the +1 480 number and outgoing calls to landlines worldwide are billed at 1:1 parity. Calls to other Iridium handsets are billed at half rate, and data calls are billed by the minute (the same as voice calls).

And with that, it's time for me to enjoy an evening walk past the Confucius Temple. Enjoy your summer, and never stop exploring!

A Counterpoint to "The Piracy Situation" (28:4)

by D351

This is going to be even more controversial, for sure, but I want to urge the hacker community to actively advocate piracy. We all think we know the moral issues, so I'm totally going to go there. However, I'm going to start with some other aspects first.

The Law is Out of Control

"Our" lawmakers have already passed a metric crap-ton of copyright laws. A lot of this happened long before online piracy. For a great example, search "Mickey Mouse Protection Act", and see what happened there. When the law was going to put Mickey in the public domain, Disney screwed the law so hard that we haven't had anything come into public domain since.

Copyright laws have been driven to the point of insanity because corporations that own content want to do everything in their power to stifle competition. If somebody is watching your daughter sing along to pop music, they aren't watching TV. Therefore, you are competition. These businesses are well aware of the fact that the vast majority of art is derivative. They are well aware that the works that an artist is most likely to be inspired by are those that they grew up with. These are the bare basics of culture. They know this, and they want to keep you from distracting their audience. Were it not for their greed, culture could evolve organically, to everyone's benefit, and independent artists would be more viable as competition.

BitTorrent could have a good reputation. It's often the fastest way to download legitimate stuff... like our own culture. But nooooo.... Now our ISPs work with these corporations to screw us out of the service we pay them for if we try to use BitTorrents... or Tor.

The Malware

The average luser these days is a joke. We (those with common sense) know obvious techniques for avoiding viruses. Still, how many hours have we wasted reinstalling a (pirated) copy of Windows (usually quicker than trying to fix it) on a relative's computer, while trying to explain that Winblows is a virus in itself and that Linux is better in every imaginable way, all because they opened an email, clicked an ad, or didn't install an update?

People don't understand that Microsoft has no sense of security and that their products are ticking time bombs for trojans. But leaving alone the fact that the Internet is full of things just waiting to destroy Aunt Gertrude's Dell, what if there were more viruses by percentage in pirated files? Who's really at fault? "You can't expect safety among criminals" may be a BS statement in the first place, but if it were the case, who put criminals in these positions? Or, more correctly, who turned people who share into criminals? Timothy Leary warned that if LSD were made illegal, people would resort to dealers with potentially tainted product. It turned out that he was right. Why are pimping and drug dealing so dangerous and profitable? Because only a criminal can provide these services (in most places). Because they've been criminalized. We should by now understand that. Your average legal and consenting prostitute does.

The Debate

Okay, when I said that I'd bring up the moral issues, I meant it. That is because I'd like to offer what I hope is a compelling argument against the idea that information is property or that shoplifting is inherently bad... or (bonus argument) that the capitalist system that is the underlying basis for all arguments against sharing is either just or natural. Perhaps if you agree with me that capitalism needs to stop, then I hope to help you explain it to others with these arguments.

Look, if I were to shoplift a CD or DVD, I'd be well aware of the fact that all of the hardware devices used to make that disc were manufactured in exploited third world countries using resources stolen from other third world countries, then transported, unpacked, and shelved by exploited wage slaves domestically. So, when you shoplift, you're striking a blow against the system that traps us in dead-end jobs, struggling to pay rent to some prick whose only work is "owning" the place (and we're the lucky ones).

The idea that sharing is stealing because the "owner" isn't making any money just doesn't hold water. What standard defines copyright "ownership?" The same corrupt laws that we all are complaining about. If I get the government to say that I own the rain, does that make it right? No, but it's happening all over the world right now.

A physical product can be "owned" because for one person to have possession of it, others must be excluded, even if only temporarily. Information only works that way in the form of secrets. Culture is not secret, and secrets that could only be justified by their own profitability are just only in the eyes of greed.

Without copyright, artists in today's society would not be able to fund their work, but how is that the fault of the people who appreciate their work? Would it not be more logical to place the blame on those that extort them (as well as all of us) out of their labor so that they can simply feed, clothe, and

shelter themselves? Perhaps the problem isn't that we're not paying for their survival but that they must pay to survive.

A Call to Action

In the states, we constantly hear of the rights of life, liberty, and the pursuit of happiness. Why is it that all of these things must depend first on our pursuit of profitability? Consider (the lilies) all of the life-affirming works these artists might produce if so much of their efforts weren't squandered in the name of profitability. Take a critical look at the garbage that the mainstream film industry produces, and ask yourself "Is the profit system working here?" Great works are achieved, not for profit, but for the sake of the works themselves, and great works are meant to be shared. This isn't just applicable to art. This goes for science and industry... and hacking. Hackers hack for love of the hack. A hacker will continue hacking if it drives them broke or gets them imprisoned.

This is because humans are meant to do what they enjoy, not what others will pay money for. What we need, as a species, is to reevaluate the system we live in. If there is enough food, why do some go hungry? If we have the technology to automate, why do some do dangerous and/or tedious work? If technology has made so much work obsolete, why do we work more hours than at any other time in human history? If we love hacking so much, why don't we spend more of our time hacking what we want to hack? I can't speak for the rest of us (or even a sizable percentage of us), but I know what I want to spend my time hacking: capitalism and government. And if I have to start by probing and exploiting weaknesses in copyright, I'm just fine with that. We could all be spending more of our time hacking. As icing on the cake, imagine what it would do to all that hard work trying to clarify what a hacker really is all about if the media were to catch wind that the hacker community is coming out anarcho-socialist!

The Piracy Situation: The Devil's Advocate

by Chip Ninja

Following R. Toby Richards' article, I felt that there were far too many anti-piracy advocates and far too little emphasis placed on the fundamental problems with the current copyright laws or the positive aspects of piracy. While initially I will be directly addressing Richards' article (as it highlights the most common views supported by anti-piracy advocates), ultimately I will get to the root of the problem.

The Law is Out of Control

While one could simply say that more laws are created due to piracy itself, this belief is simply untrue. On the surface, it appears that perhaps the current trend of adopting ever increasing copyright laws is due to rampant piracy and the millions in damages piracy causes to various (primarily entertainment) industries.

However, I would like to point out that the large corporations that are trying to "protect" intellectual property are in reality abusing their vast wealth in an attempt to extort their customers.

The first incident to highlight this phenomenon is takedown of a video posted by Stephanie Lenz, which showed her child dancing to the Prince song "Let's Go Crazy." Was the takedown filed due to copyright infringement? No, the video clearly falls within fair use. The question is, by taking the video down, how did Universal protect their intellectual property? They didn't. So why did they do it? The only plausible explanation is to show everyone who is "in charge."

However, this is just scratching the surface of the issue. Lawsuits are also common against people who mod their own hardware to work with other software (such as Geohot jailbreaking the PS3), which is also allowed by the current copyright laws. However, in many cases, when a lawsuit is filed, defendants would much rather just settle than deal with the increased legal expenses of going to court. Keeping that in mind, one could do a quick Google search and find an extensive collection of cease and desist notices threatening legal action against those who operate wholly within fair use. This practice in many ways could be compared with the despicable act of patent trolling, whereas most people look the other way simply because piracy must be stopped!

The Real Issues

What must be realized is that this is not a new phenomenon at all. Efforts were made to shut down VCRs when they first came out because "the VCR is to the American film producer and the American public as the Boston Strangler is to the woman home alone."

This thought process is very similar to the overstated belief that piracy on the Internet is destroying our entertainment industries. That is simply untrue. The real issue is that groups like MPAA have been quoted saying that they want to keep it illegal for you to create your own backup copy of a DVD simply because it creates additional revenue streams for them. Your disc gets scratched or broken, you buy a new one. You want to watch it on a mobile device, you buy the

movie again.

The question here is once you've already bought a product, why should you buy it a second time? According to MPAA, you should buy the same movie multiple times so that you have alternate ways of watching a movie - but isn't that just saying "because we want to milk more cash out of you?"

Continuing with the lost profits, let's get away from ripping DVDs for a moment.

MPAA's and RIAA's Flawed Reasoning

The highest market share for the movie industry from 1995-2012 has been original screenplays, at 48.94 percent. Remakes are sitting at 6.4 percent. Now, think back to all of the recent movies which are remakes. Since just 2008 there have been 102 remakes, whereas from 1990-2000 there were 56. So, doing a little math, we can say that from 1990-2000 the movie industry averaged around 5.6 remakes a year. The average per year from 2008-2012 is 25.5.

So in the last four years, there has been over a 400 percent increase in the number of remakes, which make up only 6.4 percent of the market share from 1995-2012. The problem is that some remakes do incredibly well, while others completely flop. The industry, however, is approaching it with more of a piñata technique - they're blindly throwing movies out there in hopes of a giant success, which simply doesn't work if you're trying to make a profit.

Does piracy affect this? Yes, definitely. Pirating a movie will certainly affect the amount of revenue generated in the box office and sales. However, there is a positive side which is often unmentioned.

The Real Impact of Torrents

Switching gears temporarily, if you knew a product you were about to buy was flawed or not really what you thought it was, would you buy it? Probably not. If you knew for a fact that your Sony TV was going to die as soon as the warranty was up, would you buy it? More than likely, you would look for a different brand. But how do you know that the new brand wasn't built the same way? You really don't. The true root of the problem is that *products are intentionally misrepresented to increase profit.* Ultimately, customer satisfaction is no longer a priority. The true priority is just to increase profit using any means necessary. The true aspect that scares big corporations about piracy is that we can, and do, use it to save ourselves from foolishly purchasing flawed products.

Let's start with what happens when a crap movie or music album is downloaded. The pirate views the movie or listens to the album, realizes that they just saved themselves at least $20, and then deletes the pirated work. They tell others that it was crap, and less people are interested. However, when a good work is pirated, the resulting word of mouth gets more people to the theater, and many pirates end up buying the work. I personally have pirated movies which have not yet been released in the United States (or ones that I am unsure of) and, as soon as I have the opportunity, have purchased the collector's edition.

Indie developers know the value of using torrents, and many embrace the idea of their work being shared on sites like The Pirate Bay because they know it will increase their exposure and thus help them more than it will hurt them. *Minecraft's* creator Notch responded to one of his fans telling him "Just pirate it" and to buy it when he could afford it if he still liked it.

So why are groups like MPAA and RIAA fighting so hard against piracy when it could potentially be good for business? They're fighting it because of what happens when a product they release is crap. Trailers are intentionally cut to make you want to see the movie. There are plenty of cases of misleading trailers, and I'm sure you can think of some on your own. Music? Only the best on the album are typically aired. So what happens when the only value a work has to offer is what is showed in a trailer or aired on the radio? Well, if you deal with pirates you know to avoid wasting your money. If you don't - well, you end up blowing your hard earned cash.

But what about the critics, you may ask. Critics and reviewers are much like politicians. Both are paid off by the media companies to write things in their favor. So, if we acknowledge the fact that reviews are often biased, what is the only true way to ensure that you have a fair assessment of a product?

That's right, you personally need to view, listen, or play it, or speak to a person you personally trust who has.

Mitigating Piracy

So, we've already established that there are flaws in the belief that piracy is a completely evil thing. However, much like anything else (such as IP lawsuits), there is a vast potential for abuse. There is no guarantee that a pirate will buy the work. However, likewise there is no guarantee that the work is even worth your money.

The true solution to piracy lies with the content creators themselves. Represent your product accurately. Stop trying to fool consumers into buying a misrepresented product and you won't lose much if at all to piracy.

Why is Piracy Still Allowed?

by jk31214

I don't want to start a philosophical debate, but I will. Why do people feel that this is a harmless crime? Instinctually, it's because, in fact, it is a *physically* harmless crime. No one gets physically hurt as a direct result of copying media. Sure, you may argue that someone put their hard earned time and money into creating it, so that hurts them financially. In the business of entertainment, when large productions are involved, these productions are invested in and budgeted well in advance by their respected production companies. Entertainers are already paid for that effort in advance with the option for royalties thereafter. It's the large production companies which stand to lose their projected profits that take the beating. Consumers put so much money into Hollywood, music, and software and have abandoned financial backing of the service industry and manufacturing. The cost of media has been trumped up so much that regular people don't even think that it's worth the sticker price that companies are asking. That's why people steal it. Just look at how we value our movie stars and music stars in this country. No other country treats their entertainers like royalty. In Plato's *Republic,* he philosophized that society created or deviated from its normal course in order to accommodate for all that was necessary, thus creating a new normal course. So, it's understandable that we have morphed into a country of audio/videophiles that elevate our entertainers to godlike status. People love entertainment and software, but not as much as corporations are asking for it. Maybe if large media production companies lowered their suggested sales prices a little, people would be more willing to pay for a CD with two good songs on it.

As far as software goes, there is not one piece of software on the market that does not have an open source counterpart. How is this possible? Do you mean to tell me that someone took their time, skills, and effort and focused them into creating software that emulates a "pay-for" application. Why the altruism? Because someone was inspired to do it, out of the search for respect? Defiance? A testament to their own skill? Who knows? Whatever the reason, we're glad that they do it. Thank you to the Open Source community! Allowing applications that people use every day to be hacked, modified, customized, and re-circulated lends itself to achieving progress more quickly and efficiently. Almost everything we use today is an improvement of something else based upon its creation in the past. Newton humbly and famously quoted an old proverb of "dwarves standing on the shoulders of giants," meaning that the dwarf can see farther, not by virtue of better eyesight, but by simply being carried higher by his giant and gaining a better vantage point. When we are free to build upon the creation of others, we can combine our collective knowledge and soar to new heights in technology and design.

Perhaps letting go of this notion of media for profit, rather than creation for knowledge and respect, will let us focus our efforts elsewhere. Profiteers for entertainment center all of their efforts into making their next dollar on a piece of work when they should be continually inspired to create for the good of the people. There is nothing wrong with expecting some compensation for your talent. But their expectations far exceed our willingness to pay for it. With a state of mind that all information is free for use, we could begin to focus our attention on manufacturing tangible goods for profit, harnessing and providing renewable resources to the world for profit, or providing useful services for profit instead of providing essentially useless and bloated entertainment for outrageous prices.

Think about the possibilities of humankind if private organizations didn't have to concentrate all of their effort on making the same products as their competitors over and over for a slice of the same pie, when each of them could just have their own pies. Put an end to antitrust, frivolous copyright infringement claims, and corporate espionage. We as a people continually reinvent the wheel, which our competitors have already invented. Not to be too far off topic, but people tend to give leniency towards piracy because it's inevitable. People already feel that there is no way to stop it, and, from their perspective, it's not that terrible of a crime. Unless heads are cut off for piracy, I don't think people will ever stop attempting to do it.

by Merl

In 27:2, there was an article entitled "My Second Implant" by Estragon, which seems to have fooled at least one person into thinking that the implant story was fact. Though that story may have been fictional, as someone with some knowledge of the current state of biotech-implants and someone who's entering into the biotech field, I can tell you that we are, indeed, not very far from the day when such implants will become possible and available. In this article, I would like to give you a very broad overview of a technology (dry-electrode EEG) which is becoming commercially and cheaply available, and which opens all sorts of exciting and fascinating doors for anyone interested in doing new and cool things involving their brain/mind. And if you are reading this magazine, chances are that you're more than a little interested in "mind hacking" of any kind.

EEG, or electroencephalography, refers to a method of recording the electrical activity of the brain by placing electrodes on the scalp, and sometimes face, of a person. The way this works is that the brain's neurons are constantly firing off so-called action potentials, or spikes, which are the electrochemical signals generated and propagated by neurons as they receive and integrate signals (spikes) from other neurons. An individual spike is too weak to be detected by these electrodes on the scalp of a person (due to the fast attenuation of the electrical field changes outside the neuron that fired), but an interesting phenomenon happens when a group of neurons is connected in a neural network - rhythmic oscillating patterns of neural activity emerge. We call these "neural oscillations" and they are a result of neural synchronization. This is a good example of what some call "emergent" behavior due to the individual nodes or neurons doing their own thing. When a large number of neurons (and such neural networks) intercommunicate, we get macroscopic oscillations that reach the scalp and can, in principle, be detected using pretty standard electrical measuring equipment. Of course, EEG recording equipment is usually quite specialized and often

contains filters (to isolate noise from the electrical grid, lights, wireless devices, etc.) and, in a lab setting, EEG recordings tend to be made by first applying an electroconductive gel on the subject being recorded, in order to get a better conductance of the signals from the scalp and to get a better recording. There is also a software processing stage where a mathematical transformation called FFT (fast Fourier transform) is applied to the raw detected waveform of a signal in order to isolate different neural oscillation frequencies, which tend to correspond to different emotional and mental states. The different frequencies are also often generated in slightly different parts of the brain, and this information is also often useful. The reason we need such elaborate methods to get good and useful recordings is that the amplitude or strength of the electrical signals that reach the scalp are on the order of 1 to 100 uV (microvolts). With such weak signals, it's very easy to get unwanted artifacts mixed in with the brain wave information. This is why in clinical settings, subdermal (under the skin) electrodes are sometimes used, where we get signals with amplitudes of 10 to 20mV, allowing for better recordings.

Now, as previously explained, lab/clinical EEGs have always tended to use an electroconductive gel and often involved the placement of ten (but sometimes up to 50!) electrodes on a person's head. This is not very convenient or wanted for a home or commercial setting. Recently, however, a company called NeuroSky released a dry-electrody technology and there are now cheap ($100) EEG headsets available. There are a number of different models by a number of different companies, but all the cheap ($100) models currently use the NeuroSky chips but offer slightly different packaging and software development kit (STKs). I will tell you a bit about NeuroSky's own EEG headset, the MindWave, as that is the one I have and the one I have some personal experience with. The MindWave is a single dry-electrode headset, where the electrode is placed on your head and there is a piece placed on your earlobe which records a reference measurement, which is important for signal filtering purposes. The unit itself looks rather good and slick, and is very light and quite comfortable. The size is comparable to a small microphone/headphone headset, except that you have one piece that sticks out with its forehead-touching sensor, and a second piece with a clip on your earlobe. Also, I should mention that the MindWave is quite nice in that it's usable with Android, iOS, Windows, and OS X. There seem to be some people who have attempted to do some things with the device on Linux, but, as usual, don't expect very good Linux compatibility. Also, the device communicates using Bluetooth. Though it may still be a little strange to walk around outside with such a headset, it is comfortable and usable in a home setting. So, you ask, "what can I do with this cool new technology?" I don't mean to sound like a sales representative for the company, but, really, you can do a *whole* lot and what you can achieve with such a technology is very much up to you - the developer, the hacker, the creator. There are a number of applications available for free (and that come with the MindWave) and there are a bunch more available in the iStore and other places online. The most important point, however, is that there are freely available SDKs and development environments so that you can write apps for your Android phones or for your home machine. These SDKs allow you to write apps in, for example, Java, and the SDK and APIs provide you with methods for retrieving the sensor values which change as your mental/brain state changes. I don't know about you, but the prospect of writing software that responds to my brain wave patterns (and thoughts) is very exciting and cool. Indeed, I suspect that most people who consider themselves "hackers" have at one point or another wondered about the brain and the possibilities that stem from using it for doing things. Well folks, the time has come and I urge you and all your friends to go out and learn things about the brain and neuroscience, and start shaping the new world that will, as Arthur C. Clarke once said, "be indistinguishable from magic." This is truly a field which awaits pioneers, great discoveries, and the creation of amazing new products.

I hope you have enjoyed this short introduction to this amazing technology and the awesome future prospects it promises. Happy hacking!

References

- http://en.wikipedia.org/wiki/➥Neural_oscillations
- http://en.wikipedia.org/wiki/➥Electroencephalography
- http://www.neurosky.com/➥Documents/Document.pdf?➥DocumentID=77eee738-c25c➥-4d63-b278-1035cfa1de92
- *Cognitive Neuroscience: The Biology of the Mind, by Gazzaniga, Ivry, and Mangun.*

Building the Better Brute Force Algorithm
A Guide to Heuristic Password Cracking

by James Penguin
jamespenguin@gmail.com

Let's begin with a brief overview of standard (non-decryption based) password cracking methods. When faced with the task of cracking a password hash, and reverse engineering the encryption algorithm used to create the hash of the original password isn't a viable choice, you are left with a couple of different options.

Dictionary Attacks

A dictionary attack is carried out by iterating through a list of words, creating a hash of each one, and comparing the result to your target hash until you find a match. While dictionary based cracking methods can be used to crack a lot of common passwords, they're not all that effective when things start to become more complicated.

Often people use one or more words in their password, and those words may or may not be separated by a space or contain numbers or punctuation. Take, for example, the password "falconpunch". It contains the two words "falcon" and "punch". Both of these words are found in a standard list of dictionary words, but you wouldn't be able to crack this password using a dictionary attack because they're mashed together to form a single "word".

We also run into the same issue with passwords that are made up of, or include, portmanteaus that are not generally found in dictionary lists. Take, for instance, the portmanteau made from combining the words "char" and "lizard". Chances are pretty good that your dictionary list doesn't include the word "charizard", thus rendering a dictionary attack not very effective for that password.

Brute Force Attacks

When dictionary attacks just won't do, you can always try cracking the password using the brute force method. A brute force attack is carried out by cycling through every possible combination of a sequence of characters (aaaa, aaab, aaac, etc.) and hashing each one until you find the sequence whose hash matches your target hash.

The benefit of using a brute force attack is that it has a 100 percent chance of success to crack your password hash. The downside, though, is that to iterate through every possible combination of a sequence of characters until you find a match for your target hash, it could end up taking a very long time, and it only gets worse the longer and more complicated your target password is.

Take, for example, the password "charizard rules". That's a password that is 15 characters long, and only contains letters and spaces. Simple, right? Well, in order to crack this password using a brute force attack, you would need to iterate through every possible combination of the letters a-z and the space character from a length of one to at least 15 characters. Let's do some math to see just how many combinations (in theory) we would have to try.

Characters	Total Combinations
1 (27^1)	27
2 (27^2)	729
3 (27^3)	19,683
4 (27^4)	531,441
5 (27^5)	14,348,907
6 (27^6)	387,420,489
7 (27^7)	10,460,353,203
8 (27^8)	282,429,536,481
9 (27^9)	7,625,597,484,987
10 (27^10)	205,891,132,094,649
11 (27^11)	5,559,060,566,555,520
12 (27^12)	150,094,635,296,999,000
13 (27^13)	4,052,555,153,018,980,000
14 (27^14)	109,418,989,131,512,000,000
15 (27^15)	2,950,000,000,000,000,000,000

That's a total of 3,067,940,118,341,250,379,359 combinations.

At a rate of testing 50 hashes per second, it would take about 1,945,674,859,424 years to try every possible combination. That's almost two trillion years!

Now, I'm not sure about you, but waiting a

couple of trillion years to crack someone's password sucks. So let's try cutting down that brute forcing time by operating under the assumption that our target password has to be at least seven characters long. That means that we only need to calculate the combinations of the letters a-z and the space from a length of seven characters to at least 15 characters. Let's see how our math looks now.

Characters	Total Combinations
7 (27^7)	10,460,353,203
8 (27^8)	282,429,536,481
9 (27^9)	7,625,597,484,987
10 (27^10)	205,891,132,094,649
11 (27^11)	5,559,060,566,555,520
12 (27^12)	150,094,635,296,999,000
13 (27^13)	4,052,555,153,018,980,000
14 (27^14)	109,418,989,131,512,000,000
15 (27^15)	2,950,000,000,000,000,000,000

That's a total of 3,067,940,118,340,848,058,083 combinations.

At a rate of testing 50 hashes per second, it would only take about 465,101,560,021 years to try every possible combination. Hooray, that's only 465 billion years, which is a lot less time compared to two trillion years!

Conclusion

From the information above, we've learned that dictionary attacks are nice, but aren't much help when trying to crack a password more complicated than something your grandma might come up with (passwords consisting of more than just a single word or that include nonstandard portmanteaus). We've also learned that using a brute force attack will (eventually) crack any target password with a 100 percent rate of success, but it'll probably take a few eons to crack longer, more complicated passwords.

So, what's a devilishly good looking super hacker to do? Why, the answer is obvious. You need to use a smarter brute forcing algorithm!

Before We Continue

You may have noticed that I've conveniently forgotten to mention anything about passwords that include numbers or funky punctuation ($, &, @, etc.). It's not that I don't acknowledge the existence of passwords like these, it's just that at this point we're only going to focus on passwords that use the letters a-z, spaces, hyphens, underscores, and common grammatical punctuation (. , ' ? !). I'll address all those kooky complicated passwords later on.

The Psychology of Password Creation

The primary issue with using a brute force attack to crack most real world passwords is that they spend a ton of time comparing hashes generated from phrases like:

aaaaaaaaa
aaacccaad
xcv hjj abu
hhgdfgdrfg

Now these are all spiffy secure passwords, but you'd be hard pressed to find someone who would actually use a password like one of these. Granted, there are a select group of paranoid types who I'm sure use passwords like these all the time, but, more often than not, people tend to pick passwords that they can actually remember; passwords that actually contain words. These words may not necessarily always be separated by spaces, be spelled correctly, or even appear in a dictionary, but they are all still at least words. They are phrases that can be read aloud, and phrases that people say aloud in their minds as they type them in.

Take for instance the words "falcon" and "punch", and all of the different ways they could be arranged to make a password. A few possible combinations would be "falcon punch", "falcon-punch", "falcon punch!", "falconpunch!", and "falcon, punch!". Looking at these passwords, no matter how they're put together, the resulting password always includes the words "falcon" and "punch", and when you read it out loud, it's "falcon punch".

So in order to crack a "regular password" (i.e., passwords that aren't random sequences of nonsense), we need a more heuristic brute forcing algorithm that doesn't waste its time on unrealistic passwords like "aaaa" and "asdxcv", but instead focuses exclusively on generating passwords made up of words that adhere to the rules of English-like words and phrases.

What is an English-like Word or Phrase?

An English-like word is a word that may not necessarily be an actual English word, but still adheres to a series of rules that our brains use to determine whether or not a given sequence of characters qualifies as a "word". Therefore, an English-like phrase is a grouping of two or more English-like words that adhere to the rules that determine whether or not a group of words qualifies as a valid phrase.

Take, for instance, this article you're reading right now. As you take in each word, your brain is running a series of tests to make sure that the word you're looking at is actually a word and not just a bunch of random letters. If I were to drop the word "kguifdgj" in the middle of a sentence, your brain would automatically flag that word as not being a valid word because it doesn't follow the "rules" of English-like words. That is, certain

rules that every word follows in order to be considered a valid word by our brains. Therefore, you would conclude that that particular sentence was not a valid sentence because it wasn't made up entirely of valid words.

So in order to create a brute forcing algorithm that doesn't waste its time on nonsense words like "sfdre" and "86ugkie65", we need to "teach" it how to perform at least some of those same tests that our brain does for us automatically so that it can determine whether a word or phrase is valid or just gibberish. By doing this, we create a brute force algorithm that only generates possible passwords that an everyday person would potentially use. Which in turn drastically reduces the amount of time spent generating extremely unlikely possible passwords.

The Rules of English-like Words

Apostrophes

A word cannot include more than one apostrophe. If a word includes an apostrophe, the apostrophe can only be positioned as the last character, or second to last character, in the word. Moreover, an apostrophe's last bordering letter must be an s.

Examples:
chuck's is a valid word
chucks' is a valid word
chuck'x is not a valid word
ch'uks is not a valid word

Hyphens and Underscores

A word cannot include both hyphens and underscores. If a word includes hyphens or underscores, the word should be split at that punctuation, and each word should be tested independently for whether or not it is a valid English-like word.

Examples:
snape-kills_dumbledore is not valid
lightsabers_are_awesome should be split at the underscores and the individual words should be tested separately to determine whether they are valid or not. If any of the individual words are invalid, then the entire word is invalid as well.

Ending Punctuation (! ? , .)

A word cannot include more than one instance of ending punctuation, and any occurrence of such punctuation can only be positioned as the last character of a word.

Other Punctuation (&, @, etc.)

A word cannot include any instances of other punctuation.

Suffixes

If a word ends in a known suffix (ing, ist, scope, ology, etc.), the last character before the suffix cannot be the same as the first letter of the suffix.

Examples:
psychology is a valid word
psychoology is not a valid word

Note: There are a very few words that don't follow this rule, like zoology. However, since words like these are the (rare) exception to the rule, it's more effective to just ignore them.

Vowels

Words must include at least one vowel.

Character Repetition Patterns

The same character can never be repeated more than twice in a row.

Examples:
books is a valid word
boooks is not a valid word

The same sequence of characters can never be repeated more than twice in a row.

Examples:
mahimahi is a valid word
mahimahimahi is not a valid word

Character Position Analysis

One of the great things about computers is that they're very good at performing simple tasks over and over really fast. Because of this trait, there are certain tests we can have the computer perform to validate words that wouldn't be efficient if you were verifying a word by hand. One such test is Character Position Analysis.

A Character Position Analysis is a test performed by iterating through each character in a word, and analyzing that character's relationship with its neighboring characters in order to determine whether or not certain characters "fit" next to each other.

To perform a Character Position Analysis, you first need to build a database that documents how often characters appears directly next to, or one character apart from, each other. This database is broken up into three separate tables that keep track of occurrence patterns for:

- the first three characters of a word (starters table)
- the last three characters of a word (enders table)
- and the characters in a word as a whole (neighbors table).

Below is an example table documenting the overall character occurrence patterns for the word "awesome". Each cell holds two numbers. The first number represents the number of times a character appears directly next to another character, and the second number represents the number of times a character appears one character apart from another character.

	A	**E**	**M**	**O**	**S**	**W**
A	**0, 0**	**0, 1**	**0, 0**	**0, 0**	**0, 0**	**1, 0**
E	**0, 1**	**0, 0**	**1, 0**	**0, 1**	**1, 0**	**1, 0**

M	**0, 0**	**1, 0**	**0, 0**	**1, 0**	**0, 1**	**0, 0**
O	**0, 0**	**0, 1**	**0, 0**	**0, 0**	**1, 0**	**0, 0**
S	**0, 0**	**1, 0**	**0, 1**	**1, 0**	**0, 0**	**0, 1**
W	**1, 0**	**1, 0**	**0, 0**	**0, 0**	**0, 1**	**0, 0**

From the data in the table above, we can conclude that the letters "a", "e", "m", "o", and "s" never appear directly after the letter "a". We can then use this data to verify whether or not other words are valid. For example, the word "amber" would be considered not valid, because the letter "m" appears directly after the letter "a" which our occurrence patterns table tells us isn't possible.

Well, obviously "amber" is a valid word (anyone who's seen *Jurassic Park* knows that), but the data we have in the table above says otherwise. So in order to perform an accurate Character Position Analysis, a very large list of words must be analyzed in order to build a useful set of character position occurrence tables. Such a list of words can be found here at `http://www.➥bsdlover.cn/study/UnixTree/V7/➥usr/dict/words.html`

Once you have a character position occurrence database, then you can perform a Character Position Analysis. A Character Position Analysis is broken up into three separate tests, and a word is only valid if it passes all three tests.

Starting Characters Position Analysis

This test is performed by taking the first three characters of a word and checking in the starters table whether the occurrence count (aka neighbor score) for the first and second characters, or first and third characters, is equal to zero. If either neighbor score is equal to zero, then the word is not valid.

Ending Characters Position Analysis

This test is performed by taking the last three characters of a word and checking in the enders table whether the occurrence count (aka neighbor score) for the third to last and second to last characters, or third to last and last characters, is equal to zero. If either neighbor score is equal to zero, then the word is not valid.

General Character Position Analysis

This test is performed by iterating through each character in a word and checking in the neighbor's table whether the occurrence count (aka neighbor score) for each character being tested and the character next to it, and the character one character apart from the character being tested is equal to zero. If any of the neighbor scores is equal to zero, then the word is not valid.

Getting More Accurate Results

One way to get more accurate results when performing a Character Position Analysis is to raise the minimum required neighbor score from zero to a higher threshold.

Rules of English-like Phrases

Spaces

A valid English-like phrase cannot include any occurrence of three or more space characters in a row. On instances of two spaces in a row, the phrase should be split at the double space and each sub-phrase should be tested separately. If any of the sub-phrases are not valid, then the entire phrase is not valid.

Examples:

"row row fight the power" is a valid phrase

"it's dangerous to go alone, take this" is not a valid phrase (because there are three spaces in a row)

Word Repetition

The same word can never be repeated more than three times in a valid English-like phrase.

Examples:

"row row fight the power" is a valid phrase

"row row row row your boat" is not a valid phrase

Phrase Ending Punctuation (! ? .)

Phrase ending punctuation may only appear at the end of a phrase.

Examples:

"zelda is so over powered in brawl!" is a valid phrase

"zelda is so! over powered in brawl!" is not a valid phrase

Commas

Commas may only appear at the end of words, and never at the end of a phrase.

Examples:

"charizard is cool, but so is blastoise" is a valid phrase

"cooking is so fun," is not a valid phrase

Words

In order for an English-like phrase to be considered valid, each word in the phrase must be a valid English-like word.

So what about those passwords that include numbers or goofy punctuation?

While heuristic brute forcing algorithms are great for generating English-like words and phrases, things begin to be a lot more complicated if your target password includes numbers or funky punctuation ($, &, @, etc.).

Going back to the topic of the psychology of password creation, remember that in general people pick passwords that are actually made up of words. Keeping this in mind, we can reasonably conclude that passwords that include numbers

and/or funky punctuation still follow this rule, but the word(s) in the password are obfuscated by these nonstandard characters. Another point to consider for passwords that include numbers only is that often they're just appended to the end of a password.

Take, for instance, the password "jalapeno". It's a valid English-like word and, using it as a base, you can obfuscate it with numbers and funky punctuation.

Examples:

"jalapen0", "jalap3no", "j414p3n0" - letters replaced with numbers

"jalapeno1", "jalapeno123" - numbers appended

"j@l@peno" - letters replaced with punctuation

All of the passwords above would not be considered valid English-like words, but under all of the numbers and punctuation, they actually are. So in order to crack passwords that include numbers and/or funky punctuation using a heuristic brute force algorithm, you need to develop a method that can mutate strings generated by the algorithm (making alterations like in the examples above) and then test all the password variants as well as the original password string against your target hash.

Are there any heuristic brute forcing programs available?

Why, yes there are! I maintain a small proof-of-concept Ruby application that implements heuristic brute forcing. See `http://github➥.com/jamespenguin/gentle-brute` for more details.

Conclusion

Heuristic brute forcing provides hackers with the ability to crack long and complicated passwords using brute force style password cracking, while not wasting eons trying unrealistic passwords.

To illustrate my point, let's pit heuristic brute forcing against standard brute forcing to crack a five character password consisting of the letters a-z.

Using heuristic brute forcing (via the Ruby program above): 517,839 potential phrases

Using standard brute forcing: 11,881,376 potential phrases

That's 96 percent fewer phrases to try using heuristic brute forcing compared to standard brute forcing!

WE WANT YOU TO WRITE FOR *2600*!

articles@2600.com

or

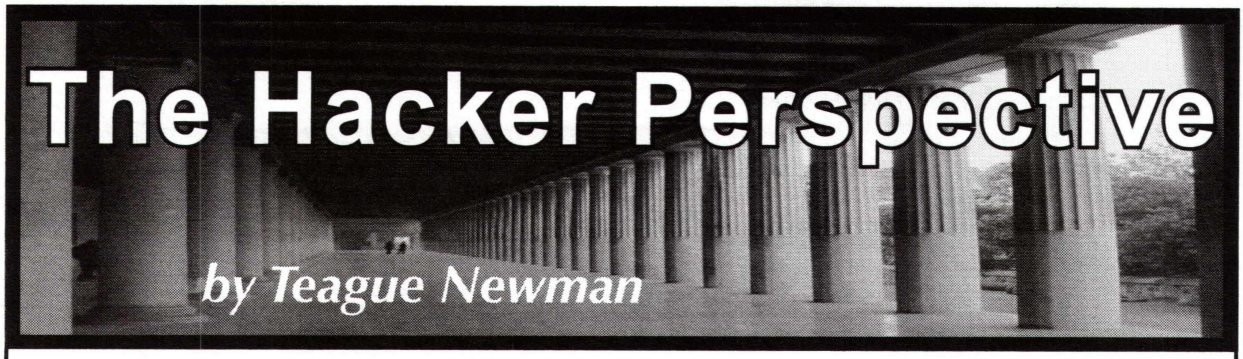
2600 Articles
PO Box 99
Middle Island, NY 11953 USA

Write for *2600* and help shape the hacker world! From the beginning, our articles have been written by people of all ages, backgrounds, and opinions. We speak with many voices and yours can be one of them. Is there something involving technology that fascinates you? Do you have some tricks you'd like to share? There are so many topics where thinking like a hacker can make all the difference in making things work better, getting around restrictions, coming up with brand new ideas...

So please send us your submissions and keep *2600* fresh. (We'll give you free stuff in exchange.) Your article can be of any length but they generally run from 500 to 3000 words depending on detail. Be sure that your entries aren't online or otherwise printed.

(Anonymity respected and protected when requested)

The Hacker Perspective



by Teague Newman

A hacker is someone who can make something work in the way they wish because they understand the "how" behind it. Physical or logical, the basis doesn't really matter. It is the desire to understand the mechanics and the process. It's the "how" and the "why" that is central to the thought process of a hacker. However, it goes beyond just being curious. It's also the implementation. Personally, I work with computers, but that is not the only type of person who I think can be a hacker. A hacker is also someone who is willing to use their end creation or modification and stand by its design no matter if it's hardware, software, or even a procedure or a philosophy.

The hacker ideology spreads much further than computer hardware and software. So often in mainstream media, the phrase "hacker" is used with a malicious connotation. This perversion of the term makes many people who truly embody what a hacker is shy away from the hacker community due to a fear of being labeled something "derogatory." Others simply feel that they "don't work on computers," so there is no way that they could be a hacker. I've met many people who would never consider themselves hackers but they truly are the essence of what a hacker should be.

Initially, I never labeled myself as a hacker because I somewhat felt the term should be earned. I didn't want to be the person that just went around saying "I'm a hacker," while having no real basis for saying so. That aside, I think I have embodied my own definition of a hacker for longer than I was willing to admit to myself. I've always tried to understand how exactly things worked. Sometimes it was out of curiosity and other times it was out of necessity.

When I was in high school, I began to care more about the details of how things worked. I can definitively recall an incident where it was out of necessity. I was doing a paper for school on my computer and it was in the 11th hour. That's when Murphy's Law kicked in. The computer bluescreened and I was unable to finish my paper. At this point, I was comfortable with computers, but not knowledgeable enough to fix everything myself. I can remember making a number of phone calls desperately trying to find someone who could fix my computer on very short notice. When I finally reached someone, I was quoted a figure of around three hundred dollars to fix the computer.... That was the defining moment where I began to learn much more about computers.

I knew that I could not afford to pay to have it fixed and I also knew that my paper had to be done before the next morning. I went to a friend's house and we began to search the Internet for information on the error. Between the two of us, we were able to determine what was wrong and devise a solution to get my machine back up and running so that I could turn in my paper the next morning. This was the point where I became comfortable with attempting to fix my own computer.

The next logical progression of this was to become comfortable working on the hardware. Once again, this came from necessity. The issue this time was that static had fried my graphics card. I decided once again to fix the issue myself and went out to the store to buy a graphics card. When I got home, I opened up the computer case and swapped out the old card for the new one. It was the first time I had actually opened my computer case, but it really was so much more than that. I successfully swapped out the card, but more importantly, I removed another barrier. In this situation, the case had always been a physical barrier between me and the actual hardware. Once I acknowledged that barrier, I was able to move past it. Previously, it had been "out of sight, out of mind," but now it was something that was within my reach and eventually led to me learning about all the components contained within.

These two events removed limitations that I had set upon myself. They were small steps, but they were confidence-builders. They showed me that working on a computer was not beyond my reach even though, at the time, it was not my primary focus. I was now much more comfortable working on and around computers. There was one more thing that really solidified my confidence and enabled me to trust myself enough to really start working on things on my own: my brother, Drew.

I can recall a phone conversation where my brother was telling me about Linux and

explaining it on a basic level. After the conversation, he sent me a few distributions and encouraged me to buy some swappable hard drives and the bays for them. With the swappable drives, I could install one or more distributions per drive and see which I liked the best. At this point, I was comfortable enough to add the bays to my own machine - and installing an operating system was not the daunting task it was a few years before.

I played with the different distributions on and off for a few months and became fairly comfortable using them. Drew now tasked me with setting up servers running certain services and left me to my own devices. There was one particularly brutal Java install that left me dumbfounded. I had asked questions to all my usual sources and could not find anyone who knew how to fix the particular issue and no one seemed to know where to look for good documentation. I called my brother, feeling rather defeated, and began asking him if he knew what was going wrong. He didn't particularly know what the problem was, but his solution was what solidified everything. I can't recall exactly what was said, but it was something to the effect of, "...be resourceful, don't just pursue your regular avenues. There is a solution out there. You just need to find it. If what you are doing isn't working, try something else until you figure out what you need." Shortly after that conversation, I found what I needed and finished up the install.

The advice was basic, but it was the catalyst that made everything mesh. I no longer felt like I would break something by opening it or working on it myself and realized that there is always an answer out there - you just have to find or create it. I now felt completely liberated. Nothing seemed out of reach. That doesn't mean everything is convenient or affordable, but the majority of the time you can figure out just about anything if you are willing to try and look for the associated information.

I now looked into everything that interested me and actively tried to gain a deep understanding of how things worked. This permeated all aspects of my life. I looked into everything from how graffiti artists gained access to some of the more obscure places, how satellite cards are programmed, and even how to reprogram the chips in friends' cars to adjust things such as air fuel ratios.

Aside from taking a deep look into everyday things, I became interested in security vulnerabilities. By this point in my life, I had many certifications from industry vendors. After going through all of this training, I had a pretty good general idea of how things should be implemented when deploying a computer or network. When this knowledge was combined with real life experience, patterns began to emerge. Many times in production environments, things are not deployed as securely as they should be. The reasons for this may vary, but the end result is the same: you are left with a vulnerable system.

In my spare time, I set up labs at home to simulate these vulnerable systems. I would then try to exploit these systems to learn more about the actual vulnerabilities as well as how to prevent them. I had a really romantic idea that maybe one day I could actually get paid to exploit systems and help show people how to secure them as well.

The idea of being a pen-tester was really still a pipe dream. I was doing general consulting on anything computer related and any security jobs I received were a bonus. I had taken the Off Sec 101 class and thoroughly enjoyed it, but just couldn't break into the penetration testing field. The problem in transitioning to the penetration testing field was how do you pitch your first test? Are people going to let you attack their network when you have no prior professional experience doing it? It was the problem of "you can't do the job unless you have experience, but you can't get the jobs that give you experience because you have no prior experience." It seemed like an impossible predicament.

And then I caught a break. In 2009, James Shewmaker ran a section of the U.S. Cyber Challenge. It was a capture the flag competition - that also happened to be free. So I enrolled. I looked at the competition as a place where I could validate what I had learned in my own lab and in the classes I had taken. As it turned out, I did pretty well and was able to prove to myself, and others, that I could actually apply these skills.

I continued competing in every round that was held, but, more importantly, a community began to form and I stayed involved. James left the network up between rounds so that participants could tinker. Many of us hung out in IRC and shared knowledge and worked on projects together between rounds. It was here that I picked up a few new tricks, and was also able to help others learn a thing or two.

By the end of the year, I had ranked fairly high in the rounds in which I competed. At this point, a handful of the top competitors were invited to Washington DC to compete in an "all-stars" round. This was great; it was the first time that I was able to meet the people that I had been competing against and working with for the better part of a year. James had also scheduled CNN to cover the event and we ended up making the front page of cnn.com.

From that point on, I was able to transition into exactly what I wanted to do. There were

people who currently worked in the information security field involved in the competition which, in turn, led to many of us getting job offers. It was no longer a pipe dream. I'm lucky enough to now be a professional penetration tester and instructor. I enjoy what I do very much and consider myself very fortunate to be able to do what was once only a "romantic idea." It seems as if I have found the perfect fit. The work I do enables me to stay on top of current industry trends and their associated vulnerabilities and the flexible schedule has even allowed me to do my own research. Being an instructor allows me to share my own knowledge as well as learn things from those I teach. My students seem to always teach me something also. There is always someone who has a rare piece of knowledge that they are happy to share with me.

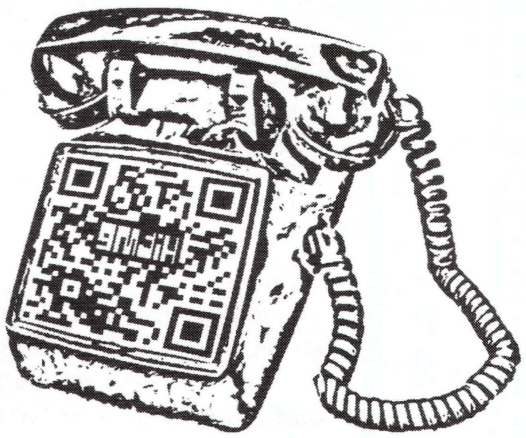
The best advice I can give to aspiring hackers is to acknowledge your barriers and go one step beyond them. If you know what is blocking you and are willing to take that first step into learning about it, you may very well find that it isn't as difficult or daunting as you may have initially imagined it to be. When you take curiosity past the point of "I wonder," and mix that with a desire to learn and the motivation to acquire the necessary knowledge, you can master anything you want.

Teague Newman is currently working out of the Washington DC area as a professional penetration tester/security researcher. He was most recently a member of a team composed of Tiffany Rad, John Strauchs, and an exploit writer who exposed vulnerabilities in the way PLCs are implemented in correctional facilities.

Submissions for "The Hacker Perspective" are closed for now, as we have enough columns for the next couple of years. But don't fret. Use that time to experiment and learn new things. When we reopen submissions, you will have a lot more to write about! But in the meantime, please send us your articles on other topics. Our mailbox is there for you: articles@2600.com

*** New T-Shirt ***

This is anything but your typical hacker-chic barcode style t-shirt. We think our deskphone image (green in color) is both pleasing to the eye and useful in a pinch. The *2600* old-school telephone logo on the back (black in color) completes the mood.



Shirts are 100% cotton and white, available in sizes S to XXXL. $20 includes shipping, except overseas.

store.2600.com

2600

or mail a check or money order to:
2600
PO Box 752
Middle Island, NY 11953
(overseas, add $5.25)

Firewall Your iPhone

by Ломика

Intro

In light of the recent CarrierIQ revelations, the feelings of paranoids everywhere have been confirmed: smartphones spy on you. What's even worse is that the data is handled by some shady company. If it went directly to the NSA, CIA, NRO, FBI, DHS, or one of our other 13 intelligence agencies, you could be more sure that they would keep it to themselves, perhaps not even allowing other law enforcement organizations access, in addition to Chinese hackers, etc. In some shady company's servers, it's free game for skilled ninjas, high bidders, and spooks of any and all varieties. Upon receiving the gift of a new iPhone 4S, I was eager to jailbreak and check for little parrots talking back to home....

Background

First, I will provide the information and background on the state of the hardware and software researched. When I received the iPhone 4S, it was running iOS 5.0.1 and a jailbreak wasn't yet available. I turned Siri on, played with it, found I didn't like it, and turned it off. This happened a few times over the course of a few days, then it stayed off for weeks. I never logged into iCloud, Facetime, and have no account for such. Never bought or downloaded anything from the app store. I never let GPS be on, and selected "Don't Send" on the "Diagnostics & Usage" settings. I, in fact, connected this phone to my computer only to jailbreak it. No sync over Wi-Fi. I basically avoided any integration of this device with others, with the Internet, and with Apple. I did have iMessage turned on, an Apple service for free texting between iDevices. I used it as a phone and a camera for this time. Here's the hardware summary:

```
Carrier          iOS version
Model            Modem Firmware
Verizon          5.0.1(9A405)
MD276LL          1.0.13
```

Fun Begins

The jailbreak (Absinthe) came out. I got around to applying it, backing up data, and applying it. It worked with no mishaps. I turned off all automatic syncing through Wi-Fi, etc. Now that I had Cydia on there, the first thing I did was the first thing any self-respecting *2600* reader would do: install MobileTerminal, network utilities, tcpdump, and all the tools one needs to take a peek at the network and see what's going on under the hood. I sshed in and got comfortable....

I understood that my Wi-Fi was at en0, and 3G seemed to be on a strange device named pdp_ip0, of which there were four, as follows:

```
pdp_ip0: flags=8051<UP,POINTOPOINT
➥,RUNNING,MULTICAST> mtu 1450
inet 10.255.255.156 -->
➥10.255.255.156 netmask 0xffffffff
pdp_ip1: flags=8010<POINTOPOINT,
➥MULTICAST> mtu 1500
pdp_ip2: flags=8010<POINTOPOINT,
➥MULTICAST> mtu 1500
pdp_ip3: flags=8010<POINTOPOINT,
➥MULTICAST> mtu 1500
```

Above the 10.255.255.156 would be your mobile broadband/3G IP address. The 255s were placed there in the same manner that phone numbers in movies use 555. Now with this information, I could cap packets on the 3G or Wi-Fi side, and I knew the IP addresses. I ran tcpdump on the thing while it wasn't in use, and saw some packets that seemed unexplained, so I started messing around with netstat, running `netstat -n` to see what connections were happening and what status they held. I didn't like what I saw:

```
Active Internet connections
Proto  Recv-Q  Send-Q  Local
➥Address Foreign Address (state)
tcp4   0   0   10.255.255.156.49159
➥198.224.191.68.143 ESTABLISHED
tcp4   0   0   10.255.255.156.49158
➥17.172.232.51.5223  ESTABLISHED
tcp4   0   48   192.168.1.8.22
➥192.168.1.3.41445  ESTABLISHED
udp4   0   0   *.*   *.*
```

The first two connections, as you can tell, were on the mobile broadband. Mind you, this was happening while I had an excellent Wi-Fi connection, which you can see me sshed in over on the third line. You can see that I had an established tcp connection through my 3G hardware to these two mysterious IP addresses. I looked them up. The first range was owned by some company unknown to me (`http://wdspco➥.org/`), which owns the range 198.224.0.0/16. The second was Apple: 17.0.0.0/8. So time went on, and I kept an eye on this. It seemed to be the status quo. The phone was *always* connected to some IP in Apple's range on port 5223, and in wdspco on port 143.

The wdspco IPs didn't seem to be allowing outside connections from my home cable, either. But they were happy to let my phone connect. Wdspco seems to lease IPs for mobile devices, so it's also likely that whoever this is is simply leasing these addresses from them. Either way, a telnet into one of their servers from my phone yields this welcome message: `* OK Proxy➥IMAP ready to serve you, master.`

I looked online and found others complaining

about this same thing - not even about possible privacy "issues," but about losing bandwidth that they paid hard earned money for.

So What Are They Sending?

Now that it's established that there are little tweets going back to Apple, we must ask: "What are they sending?" I can't answer that question, but I can address whether or not these things are data or simply pings. First of all, it is important to note that the communications to Apple often come as a cluster of three packets every five minutes or so. The first sends 85 bytes of data from the phone to Apple. The second is about 37 bytes of data from Apple to the phone, totaling about 93 bytes. The last has no data, totals about 56 bytes in size, and is sent from the phone. This seems to be the standard interaction. The data fields do not stay constant between these clusters of communication. In our limited observation of these exchanges, one larger packet was observed being retransmitted many times. It contained a plaintext string `courier.push.apple.com`. I looked this up and saw that it had to do with Apple Facetime, a video chatting service. A service I have turned off. I checked online to find that other people have been complaining about not being able to turn this off in desktops and laptops.

After a few days, I came to find that this traffic was largely due to iMessage. I decided to play with this, and found that the range 198.224.0.0/16 was associated with iMessage, but not necessary for functionality. I also saw some of the same connections even with iMessage off. It is also noted that when changing iMessage settings, I saw brief connections to the range 63.116.166.0 - 63.116.166.255 on port 80/tcp, which is Akamai. Akamai is a data collecting kind of company - I have no need for them myself.

Either way, it's clear that this traffic was largely unsolicited by me, and has proven to be difficult or impossible to stop in settings. Even with iMessage off, these connections were still forming, and some of them weren't necessary for iMessage in the first place. To me, this was a problem and required some fixing....

Solution - OpenBSD pf

I came to find that the "OpenBSD pf" packet filter was built in and installed, along with its relevant control pfctl. I decided to block all traffic from Apple, because I really just didn't need them for anything, other than this beautiful hardware I had. After messing around and reading man pages, I ended up with this pf.conf:

```
3g = "pdp_ip0"
wifi = "en0"
apple = "{ 17.0.0.0/8
➥ 198.224.0.0/16
➥ 63.116.166.0/24}"
set block-policy drop #play dead
set skip on lo0
block in quick on {$3g,$wifi}
➥ from $apple to any
block out quick on {$3g,$wifi}
➥ from any to $apple
```

This, as you can see, simply blocks the offending IP ranges. Put this in `/etc/➥ pf.conf` and, to start pf, run `pfctl -ef ➥/etc/pf.conf`. The packet filter was enabled, and I went back to playing with `netstat -n|head`. At some point, I noticed something I found quite amusing:

```
Active Internet connections
Proto  Recv-Q  Send-Q  Local
➥ Address  Foreign Address
➥ (state)
tcp4  0  0  10.255.255.156.49366
➥ 17.172.232.93.5223  SYN_SENT
tcp4 0  0  10.255.255.156.49365
➥ 17.172.232.220.5223  SYN_SENT
tcp4  0  0  10.255.255.156.49364
➥ 17.172.232.147.5223  SYN_SENT
tcp4  0  0  10.255.255.156.49363
➥ 17.172.232.163.5223  SYN_SENT
tcp4  0  0  10.255.255.156.49362
➥ 17.172.232.159.5223  SYN_SENT
tcp4  0  0  10.255.255.156.49361
➥ 17.172.232.83.5223  SYN_SENT
tcp4  0  0  10.255.255.156.49360
➥ 17.172.232.141.5223  SYN_SENT
tcp4  0  0  10.255.255.156.49359
➥ 17.172.232.140.5223  SYN_SENT
```

Ahahahahahahaha no one can hear you scream little birdy - all your SYNs are going to /dev/null!!

This persisted for some time. Here and there, I would check and see this SYN gasping. But it seems to have died off now. I went to figure out how to add this to the boot sequence, and found `launchd.conf`. I added the line:

```
bsexec .. /sbin/pfctl -ef
➥ /etc/pf.conf
```

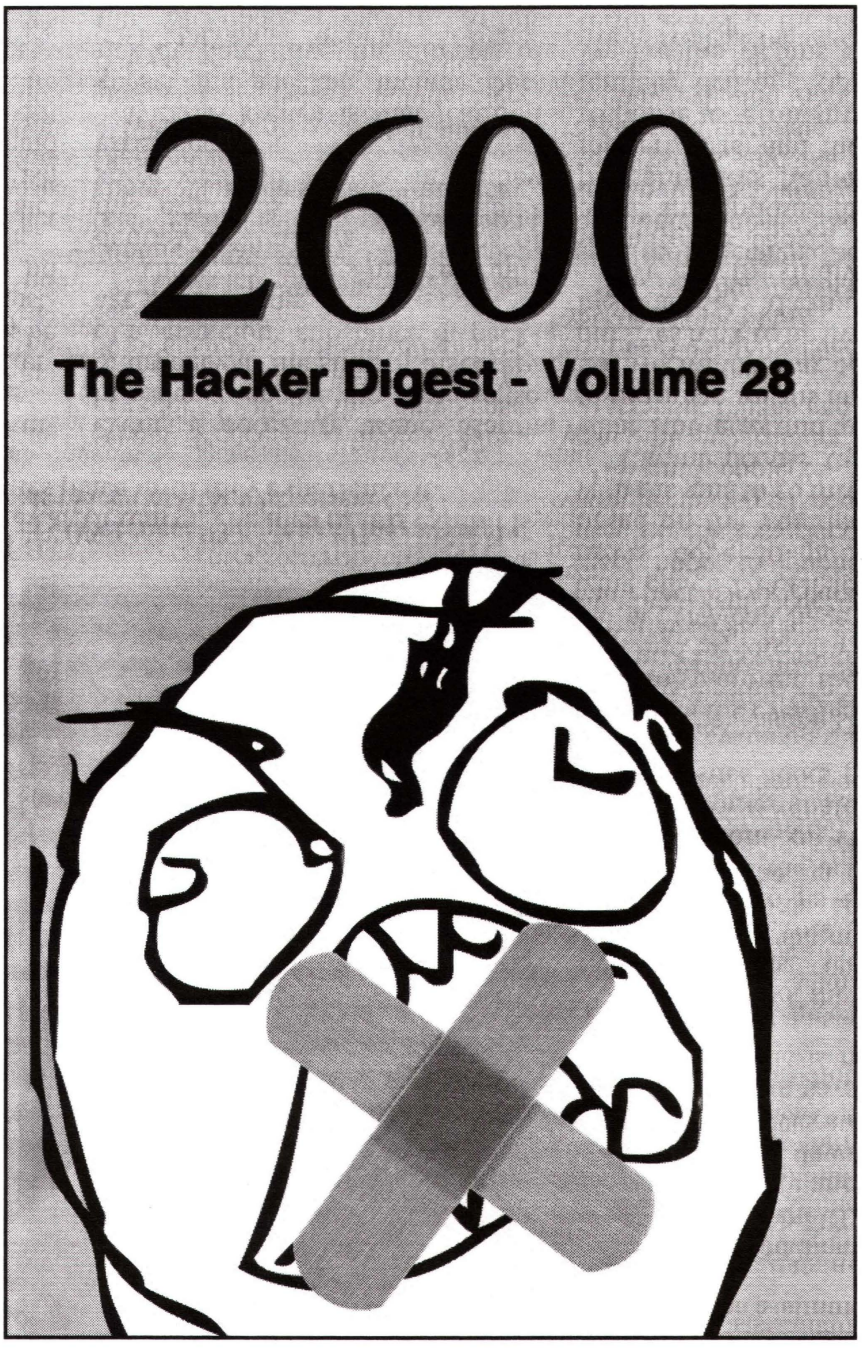
Now it starts at boot and loads the configuration. To turn it off, use `pfctl -d`.

Conclusions

My initial observations were tainted by iMessage, but further observation of this behavior was made with iMessage turned off. Apple, and three other entities that are not entirely clear, had unsolicited connections opening from the phone to servers out on the web. One was onto a hidden IMAP server, another was to Akamai. This means that there is software making these connections. I am sure some of it, or all of it, is built into the firmware. The easiest way to deal with this is to just block the hosts. This may get tricky, depending on which services you would like to use. And as always, further investigation is warranted. The future is written by you.

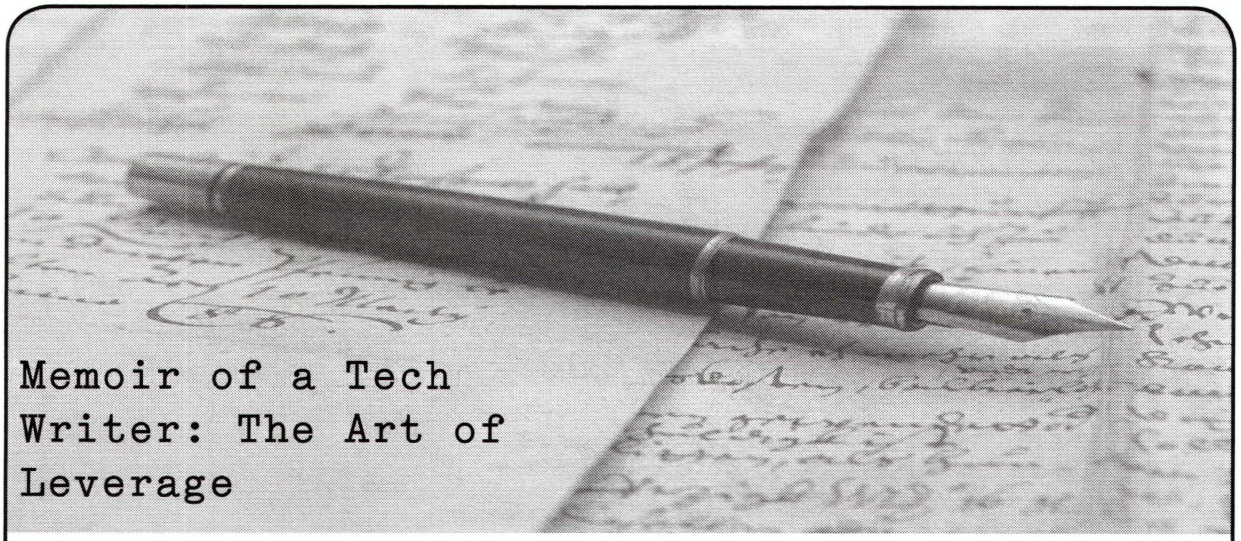
Gr33tz to callz, lace, лази, s4m, and ptq.

It's Here!



Now available online in PDF format
and for the Kindle and Nook!
All DRM-free, 282 pages

store.2600.com



Memoir of a Tech Writer: The Art of Leverage

by ellG147

When you're a freelance tech writer, projects come in all shapes and sizes. You never know what the next challenge will be, but you can count on the likelihood of dealing with language and cultural issues since more U.S. tech companies are outsourcing or partnering with companies overseas.

When I was asked to edit a post-translated software manual originating from Europe, I realized I was going to have to do some planning and preparing, especially since I would be working with people whom I didn't know. So I conducted an informal analysis of the people I would more than likely be collaborating with learning about their preference(s) of communication, daily and vacation schedules, depth of knowledge about the project, and so forth.

And since I was the new kid on the block, I realized it wouldn't hurt to apply some simple psychology (social scaffolding), so I placed a candy bowl and jar of interesting rocks on my desk to develop an instant rapport with coworkers. Additionally, I let people know that I took the liberty of putting together a photo stock (testing out the company's digital camera equipment) that could be used for recruitment flyers or slide show presentations or other. You'd be surprised how many people took me up on the offer. People are always in need of new photos from a fresh perspective because it makes them look good.

In regards to companies, I've found throughout the years that there is usually a very small percentage of people who are willing to help you by being forthcoming with information, guidance, and resources. Conversely, there are those who help but it is like pulling teeth, or those who will give you just a smidgen of their time because you're on the meter. In regards to departments, they can be very protective of information and may or may not share information with other departments.

Once I had a general idea of my people resources, I asked myself this important question: Was this manual/software someone's pet project? If so, whose? This is an important thing to find out if you can so that you can immediately align yourself with this person or persons. Ask the individual(s) whose pet project this might be for their help and assistance whenever needed - and for as much insight as possible. Knowing whether a product will be used primarily as a research tool can make a huge difference in the way a manual is slanted.

Don't hesitate to cc your PPP (Pet Project Person(s)) should things bottleneck or you discover a weak link in your people pool so that you can keep steady, forward progress with your project as some people tend to procrastinate or have other issues. If your PPPs are up there in the chain of command, this gives you additional leverage. Use it, but don't abuse it.

A critical decision that needed to be made was how deep to go with the edits of the manual. Since this particular project involved sociopolitical considerations, things could get rather sticky. The company who hired me did not want to step on the toes of the developers who wrote the manual, as this might jeopardize work relationships. However, the manual needed to be improved upon and brought up to the standards of the company who hired me. So what does one do in a Catch-22 situation? Work in a gradual rapport with all parties concerned and exercise tact. Let people know your intent and reasons for doing what you're doing so that there's no room for misunderstanding. Use phrasing like "...requires some fine-tuning" as opposed to "...requires a a major overhaul."

Since we live in a make-work universe, debating whether to start the manual from scratch or fix the existing manual would both have their challenges. I chose to work with the existing

manual mostly because the developers had already deposited a great deal of energy into the project. In this case, my choice was based upon a matter of respect.

After reading the first few pages of the manual, I experienced what I call psychological entropy: difficulty in getting through just a few pages without developing a headache due to transposition of words, translation issues, run on sentences, misplaced or lack of articles, improper gerunds, odd word usage, and so forth. Since getting through the manual was extremely difficult, I decided on a different tack with the goal of making the manual more readable so that more critical editing could take place later.

My first step was to find out if anyone in sales or marketing had already slogged through the manual - in its current condition - as a foundation for developing training or preliminary marketing materials. If so, perhaps various incarnations of a GO TO reference was already available albeit in the form of rough notes stapled together or text files or other. If not, then I could at least query these individuals to garner insight.

My second step was to gather background info on the developers by talking to key individuals in the company who actually met them at various company meetings and so forth. Based on the developers' personality types (in this case socializers), I looked for probable areas of strength and weaknesses in the manual. Fortunately, I had worked with socializer types in the aviation industry and this provided me with an a priori reason for coming up with probable scenarios in relation to software.

After steps one and two, I proceeded by spot checking the manual while working with the accompanying software, taking down copious amounts of notes, page numbers, etc. I found enough concrete evidence to support the personality-type theory and this made it possible to roughly gauge how long it would take to fix various areas in the manual along with their code-dependencies. Ultimately, I was able to come up with a viable work plan (as enumerated below) that would help me accomplish the goal of making the manual more readable.

Work Plan

0. Review images and charts and tables. Fix any glaring errors in the tables, charts, images. Get updated visuals if needed. Send request promptly to the necessary parties.

1. Take care of the technical material: check with resource engineers about part numbers, system offerings, transformers, proper cables, EMF issues. Revise chapters and paragraphs and captions and images.

2. Review chapter on installing the software and troubleshooting. Consult the software engineer in sales or support or other.

3. Remove all marketing content/braggadocio. Use FIND and REPLACE menu options to expedite cleanup of misplaced words and missing articles, improper gerunds, contractions, etc.

4. Embellish where lacking (click tabs in software to see what you get and see if this is written up in the manual). Also, are these screens included in the manual - and should they be? Or should they just be written up in paragraph form?

5. Carefully review chapter on modes of operation of the software. Is it clear and correct and does it contain a logical flow? Spend a good deal of time on this core chapter and use it as a paradigm for the rest of the manual. All pertinent information should be grouped into paragraphs and not scattered about.

6. Review the safety instructions. Make sure they are correct and complete and repeated in areas where needed because of liability issues. Have resource engineer review this section as well to be sure material complies with U.S. standards and laws.

7. Add more images where it would help to clarify the text. Set up photo session at the end of each work week during early morning hours. Use internal resources as subjects.

8. Get a perspective: print out various pages or chapters and have others review it and provide feedback based on a questionnaire that will be provided. Rework areas based on feedback. Keep all questionnaires and use as testimonials (if needed).

9. Convert manual to plain text and specified font type.

10. Have QA and select others in the company to review and critique the manual once again. Print and bind. Provide questionnaire.

After each milestone, I sent email updates to targeted individuals to let them know the status of the project as well as to demonstrate progress and to elicit early feedback.

Once the manual became more readable, it made it easier to determine what needed to be done to bring the manual up to company standards.

At this stage of the game, I never hesitated to ask myself what I needed to do to work harder at bringing to fruition my secondary, tertiary, and quaternary goals for the project.

Finally, when the manual was near completion, the people who were extremely helpful with the project received positive feedback and a note of gratitude. Their supervisors also got wind of their cooperative demeanor.

Missing Issues

Dear *2600:*

Went to the meeting - it's right by the university. I was the only person there. I just had some Russian sounding guy asking me to fix his computer (which I did because it was simple and I needed to finish my coffee). Then I asked around the store where the newest *2600 Magazine* was so I could buy it. Needless to say, they told me they did not carry it at all, and have not for a while (very disappointing). I have heard of a hackerspace here in Las Vegas. Maybe you both can team up or something. The Barnes and Noble location seems dead.

Dedicated *2600* Reader
James

We spoke with a manager at this very store and she not only confirmed that we're still carried, but was able to find several issues on the shelf. If the meetings are no longer happening at that location, we'll delist them effective next issue.

Dear *2600:*

Just stopped by my local Barnes and Noble (that I've been getting the mag from for years) to pick up the latest copy of the zine, only to find it nowhere to be found. I clutched my chest as my heart began to race and I felt the walls close in on me. I raced to the counter to inquire and get a shot of customer service to cure my panic attack and get my latest hacker fix, hoping it would just be a quick trip down to the bowels of the store past the wall of lost magazines and into the hall of literature that scares old ladies to retrieve my copy of *2600*. But after consulting the archives on his 486 and after ten minutes of buffering, I was told that they don't carry the mag anymore. Well needless to say, the paramedics came and, long story short, I renewed my subscription after quite a lapse as (after checking for the past two issue releases at two stores) I can't seem to find any more stores that carry it in my area. So question time: is there something going on with the magazine or your publishers as both Barnes and Nobles I checked at said they don't carry this magazine anymore. I'm sure it's just a matter of time before an online only switch, but I just wanted to let you know that my old routine of going to the local store, getting my 100 dollar coffee, and my latest *2600* will now have to be changed to a walk out to my mailbox in my boxers with a cup of that crappy homemade coffee with no logo to show off to strangers on my cup. You may be asking yourself what the point of this letter is and I asked myself the same thing. Best I could come up with was that I still enjoy being able to pick up a copy of the mag in stores, so I'm putting in my vote for keeping the rag in as many stores as possible and asking if there's anything I as Joe Reader can do to keep it in stores? Keep the mag in stores and keep me away from the outdoors in my boxers.

Enygma

We do seem to be getting a disturbing number of similar reports recently. Yet our distributor tells us that we should be in every Barnes and Noble without fail. So, if such a thing happens in the future, please let us know the exact location of the store in question and, if possible, the name of the person who told you they no longer carry us. There are just too many of these reports coming in for us to be able to dismiss this out of hand.

Dear *2600:*

I have been a regular reader of *2600* for over two decades and have never had any trouble finding the current issue of my favorite quarterly in the physical paper form until recently. I have always bought the current issue at my local magazine store or at Borders, but both of these outlets recently went out of business. So I found myself looking for a new place to cop *2600*. I went to two Barnes and Nobles in lower Manhattan: the Union Square store and the 18th Street and Fifth Avenue store. Both stores had an extensive magazine section with every computer and technology magazine I could imagine except for *2600*. I am well aware that *2600* is available for the Kindle and other digital formats, but I am

old school and want my *2600* in the traditional physical paper magazine format. Could you look into why Barnes and Noble and local magazine stores in New York City no longer carry *2600?* If you contacted them and made them aware of the demand for the magazine, I'm sure they would be willing to stock *2600* if they no longer carry it or would carry more quantity of the current issue if they sell them out so fast that there are not enough copies to meet the demand for them. It is an outrage that I can no longer obtain my precious quarterly issue at a local outlet. I have spoken to others who have experienced this same issue and they too want to be able to pick up a physical issue of *2600* at local stores again. Please look into this and resolve the issue to the readers' satisfaction, as denying access to the best intellectual/technology quarterly to those who must have it is a tragedy. Thanks for the best magazine ever!

Brainwaste

Again, we seem to get conflicting answers from the various bookstore employees. We definitely should be in both of those stores. Ironically, we get notices of returns (unsold copies which actually are never returned) from these very locations. Perhaps they are never being put on the shelves in the first place. The only way to find out what's going on is to see exactly what an employee is referencing when they conclude that we're no longer being carried. Anyone who experiences such an issue should find out who they spoke to and let us know all of the details. Please be nice to the employees as they are the ones who will ultimately help us figure out just what's going on.

Dear *2600:*

From inside the bookstore... or why you're hated for hacking:

This piece was inspired from some comments that I read in the 29:1 issue of *2600*. Some misconceptions I deal with daily as a manager for Barnes and Noble leapt out at me. First, get the name of the store right. Nothing kills your cred quicker with a retailer than slaughtering the name of the company they toil away for. It's not Barnes and Nobles. There is no pluralization unless you happen to visit two stores at once. You are standing in Barnes and Noble. There is the other problem. You probably aren't standing. You are probably laying on the floor with a pile of PC mags you do not intend to purchase and some networking manuals you just plan to snap some pix from. It's not a library, contrary to popular belief and urban legend. It's a retail store. When you lay on the floor, you make my taking a header a constant possibility, but more often than not you're just in some old lady's way and she has to beg you to shift your lazy ass over so she can get her book. You know, the one she came to actually buy. Then the Starbucks thing. There is no Starbucks inside the Barnes and Noble. There are cafes. Cafes that serve Starbucks' product. Just like we serve Godiva and Cheesecake factory product. There are no magazine managers. There used to be magazine leads, which were employees that made 25 cents more than your basic everyday bookseller because they could sort periodicals just a tad faster than average. You may not find *2600* because we only get so many copies per location and trust me when I say we are talking about single digits. You may also not find it because a fellow hacker snuck it into his backpack while in the cafe, in the restroom, or while laying on the floor. Sure, it could also be buried behind the comic books or *O Magazine*. Just don't blame the employees. Blame the last kid who stuck it there instead of where it went and then hope the employee assigned to clean up the hundreds of magazine titles hasn't flipped out yet because of the total mess people leave in that section. We don't dislike hackers. At least, not all of us. In fact, many of us, based on the very liberal definition supplied regularly by *2600,* are indeed fellow hackers. We hack our intra-net systems daily. We hack our Nook tablets and freely share our knowledge with anyone that will listen. You could quite possibly host a *2600* meeting in any of our stores if you just temporarily turn off the sometimes myopic view of you versus us and realize the ground rules are kinda simple. One, be a customer. Not a loiterer. There is a difference. People tell us all the time, "I'm at Barnes & Noble *all* the time." So am I. But, I'm an employee. What's your excuse? If you are sitting in a place of business for hours, using their products and resources, and not contributing in any financial sense then you are *not* a customer. For the love of Linux, at least buy a coffee. Make the effort. If people treat us like a library, I have news for you, eventually we will also start to fade away like they have. Brick and mortar retailers need a revenue stream to stay open, folks. Two, and this is something I believe *2600* regularly espouses, make sure your meeting is open to everyone and anyone. One thing we do not tolerate is exclusion. Lastly, just be a human being and speak and act with a modicum of respect. If you spent your day working for a company that offers over 2.7 million books and every half hour some knucklehead came in and said, "I'm looking for this book. I'm not sure of the title or the author. I think maybe it had a red cover!?!", you'd appreciate someone that appreciated you. Lastly, here is the trick to finding *2600* and getting the info and assistance you need. Ask to speak to a

manager and keep in mind that just like all other people and professions, there are good ones and bad ones. I'm typing this in OO.o Writer on my Easy Peasy Linux box and I'd love to show you how to tweak your N2A card to best take advantage of all the hidden hardware potential of your NookColor. Ask the next guy, and he might think *2600* was a gaming platform he played Pitfall on as a little tyke back in the day. Just keep asking questions until you find the person in the store that knows what you're talking about and don't assume everyone working there is a retail zombie or a total tool and I swear, we'll afford you the same respect. Peace, love, and lines of code.

BookeeNookeeLookee

First, you're in serious need of a vacation. Second, thanks for the tips, but it really shouldn't be as hard as it's become recently. An employee should be able to answer a simple question, such as whether or not a particular publication is carried by the store. If they can't, it's up to them, not the customer, to find someone who can help them. It's really impossible to say how our issues get hidden or misplaced, but it shouldn't be a mystery to let people know that it is in fact carried and, assuming there's some sort of inventory system in place, whether there are any issues left. Barnes and Noble actually charges us for lost issues as if it's somehow our fault when they go missing inside the store. Yet they repeatedly refuse our offers to have our trained guards stationed by the issues to watch over them around the clock. It's easy to blame the customer for the problems, but seeing as how they can't even get a straight answer as to whether or not our magazine is carried in particular stores, it's hard to believe that the fault doesn't sometimes lie elsewhere.

Questions

Dear *2600:*

I'm a journalist working out of Albuquerque, and I'd like to cover the HOPE Number Nine conference in July in New York City. Just getting there will be financially painful, so I was wondering if there were any press incentives afforded in exchange for publicity. I realize mainstream publicity isn't the goal of *2600* or the loyal masses comprising the base of HOPE; fortunately I don't write for a mainstream publication. The *Local-iQ* and *BoundByTape* are both homegrown arts and entertainment magazines published out of Albuquerque, a city long known for its tech-savvy citizens. The conference would make for a great story, and I'd love to be there; HOPEfully you can help make this happen.

C.

Yeah, here's the thing. If all of our speakers, attendees, and participants of every other sort can find a way to get to the conference, we expect interested journalists to be able to do the same. We don't believe in buying publicity regardless. It always manages to find us for free.

Dear *2600:*

I'm a happy Miami subscriber awaiting my first issue. I also ordered the past five years. Is it possible to keep ordering five years at a time and when I reach 400 dollars you send me a reminder? My wife was not too happy with the 100 dollars I spent, nor with all the Atari 8-bit stuff I have. Regardless, due to lack of funds and to keep her mad at only 100 dollars a time, it may seem like a good idea. I also purchased the Collector's Edition of *The Best of 2600*. I'm a bit OCD, so I can't help myself with books and old equipment. By the way, when I received my five years of back issues, I was hoping for an additional surprise. While no surprise, the letters to the editor are my best late reading I ever had.

Finally, I'm hoping to start a *2600* meeting down here in Miami. I have already emailed a place to see if it was OK with them. Do you think it is better to ask the coffee shop before or just show up to make the meeting? I'm following your guidelines 100 percent. I would like to make a call to all *2600* South Floridians to be ready for the meeting we will be having. I'm hoping to see people at the meetings including anyone not from earth. We are free, and here to stay!

Bluz

Well, let us know if any aliens show up. We find it's best to test out a prospective meeting place with a few people to see if there are any issues with groups. If you want to get a place's blessing, you'll usually get a positive response. Regarding your back issue order, we do try and enclose something extra in every order but sometimes we might miss one. We apologize for that. We really can't monitor your 2600 habit and cut you off at a certain amount. Perhaps there's an app for that?

Dear *2600:*

I recently asked myself what is it that I really want. This is what I came up with: I want to be like Ricky Greenblatt, Bill Gosper, Stew Nelson, Allen Baum, Stephen Woz, Nikola Tesla, and Holmes. What makes me most happy is when I find an elegant solution to a problem. I only wish I could learn faster.

Love the mag. Keep it up

Dave

It'll be most interesting to see how you turn out.

Dear *2600:*

I don't know as much about computers as you guys do but I need your help. My host file has

been hijacked. I don't know how or even who! But when I look at my netstat when I surf the net, it says *www.007guard.com 127.0.0.1*. No matter what anti-virus, anti-malware, and firewall programs I try, nothing works. It's still there and when I cloud surf, it's still there! Please tell me how to get rid of it. No one else knows how. Please email me back and tell me how to get rid of it!

Phillip
Florida

First off, you somehow have reached the impression that we're some sort of help desk. Let us assure you we are not. You won't be receiving an email from us explaining how to fix this problem. However, since we're a magazine, we have just printed your letter and will now answer it inside our pages. We trust the wait of several months has not proven too agonizing.

This is actually not an uncommon problem. You simply need to edit your hosts file (not knowing what operating system you're running makes it hard for us to tell you exactly where that is, but a Google search will turn up that information) and add "127.0.0.1 localhost" to the very top of that file. Apparently, that somehow got deleted and the next line presumably contains a line that reads "127.0.0.1 www.007guard.com" which has the effect of mapping your localhost to that site, which was added to your hosts file as a site to block. So, when you run netstat, you wind up seeing that domain every time you should be seeing localhost. The short version is that there's nothing wrong with your system and adding that line to the top of the file should fix it.

Not bad, considering we're not a help desk.

Dear *2600:*

I recently subscribed to *2600,* but I already have quite a sizable amount of your editions. I'm trying to find an article you guys ran off between Volumes 19 and 24 (that's the most I can really narrow it down to). It was about how printers are a weak point in a network. I recall that it referred to using nmap to determine the OS of the printer, then somehow giving it a lot of print jobs, effectively creating a DoS. I really would like to find this article again but I'm not getting any luck. Anything you could offer would help.

Ulysse Carion

We think the article you're looking for is called "HP Printers: The Hidden Threat," which appears in our Spring 2005 issue (22:1). At the moment, the best way to search for old articles is to use the search function at store.2600.com. As more of our back issues become digitized, this process should become even easier.

Dear *2600:*

First off, I am a massive fan. *2600* is my favorite piece of hacker literature. I recently built a new blog which is pretty similar, I suppose, to *2600* in terms of the types of pieces that go up. It's still being populated with content before any promotion of the site. I just finished Volume 29:1 and there is a piece in it called "The Hacker Perspective" by ternarybit that I thought was just stellar. I would love to post this article word for word on my site while another contributing writer is finishing his piece, with full credit to ternarybit and the source being *2600,* with your and his/her permission of course. It really would mean a lot if that's possible. Thanks in advance.

Legacy

That's not a problem as long as attribution is given.

Dear *2600:*

I was planning to go to a meeting of *2600*, but I'm from Belgium. Well, technically, this is no problem. Three hours with the train and I'm in Utrecht (Netherlands) for the meeting there. But the train is not very cheap, so first I really wanna be sure that this meeting still goes on. Can you please assure me that there will be somebody there? Because I'm not gonna go so far from home for nothing. I'm hoping for a reaction.

Roel

Our reaction to this is to advise you to just go, and possibly bring a friend or two. Let us know if nobody else shows up so that we can correct our listings. And if there is a meeting, or if you wind up breathing new life into an otherwise defunct one, let us know that too. Email meetings@2600.com to send your updates.

Defeating the System

Dear *2600:*

An application for a silly part-time job (one cannot live on hacking alone) asked for a typing certificate that proves that I can type at least 50 words per minute. Use any web based certification services, they said. A quick Google search found a multitude of sites with names like typingcertificate.com that for a mere seven bucks promised to give me a five minute typing test and provide me with a beautiful official looking certificate of my achievement. I started the test which had a text display field on top and an input area - which looked liked a regular html input type text area - below. But who wants to sit there and type for five minutes? Could I just do a simple copy-and-paste from the text display field into the text input field? Would they be dumb enough to allow this? Yes and yes, it turns out. And so, I am now a proud owner of an official certificate which says that I achieved the

speed of 289 words per minute at 97 percent accuracy (this last number is a bit puzzling - I did the cut-and-paste of the entire text so I should have 100 percent accuracy). The website told me that among the 1600 people who took the test my result was the seventh best. Makes you wonder if the other six guys discovered the copy-and-paste shortcut faster than I did. Also, how many similar "certification" sites have the same "feature?"

I worried a bit that the 289 WPM made me a typing Einstein (or a circus act) and that people may want to actually see me performing such a trick. So I took another test (the seven bucks buys you two attempts) but this time I calculated the number of words, divided that number by 60 (60 WPM sounded like a normal, safe typing speed), and waited the appropriate number of minutes before performing my copy-and-paste trick.

Full disclosure - I can type at 50 WPM with my eyes closed (well, almost) so I did not cheat on the job application, if anybody actually cares about this.

Greg

While this is a neat (and unbelievably simple) trick, we suspect the people behind it believe anyone presenting a certificate with such superhuman abilities will soon find themselves tested by their employers and will henceforth learn a valuable lesson about honesty worthy of an Afterschool Special.

On Piracy

Dear *2600:*

Copyright laws were never about intellectual property, it was all about power.

For example, look at the Megaupload situation. Megaupload was a file upload service. On December 9, 2011, Megaupload uploaded a company promotional video named "The Mega Song" to YouTube. The animated video featured appearances from Chris Brown, Will.i.am, Floyd Mayweather Jr., Kanye West, Jamie Fox, Serena Williams, Kim Kardashian, The Game, Ciara, Printz Board, Kim Dotcom, Lil John, and P. Diddy over a song by Printz Board, Kim Dotcom, and Macy Gray. Even though Universal Music Group (UMG) did not own the copyright to any part of the video or song, UMG sent a request to have the video taken down. YouTube complied with their wishes.

At the time "The Mega Song" takedown took place, Megaupload was going to relaunch Megabox. Megabox was a legal, free music service which would allow the artist to receive 90 percent of all revenue. This kind of service would allow more profits for artists and no control from the music corporations. On January 19, 2012, Megaupload's website was taken down, even though they complied with every DCMA takedown request. Their CEO, Kim Dotcom and several employees were arrested. All access to content from the website, legal or not legal, was taken away.

Unfortunately, that's not the only case of corporations trying to take control. The United States Congress, bribed by the entertainment industry, was pushing to pass the Stop Online Piracy Act (SOPA) and PROTECT IP Act (PIPA). Both laws, if they were passed, would give corporations the power to censor any part of the Internet without trial or reason.

The Internet is not the only way corporations try to take control. They also try to control your personal devices. In 2005, Sony BMG shipped CDs with rootkits which created vulnerabilities for other malware to exploit. The rootkit was installed on many ignorant consumers' computers who believed they would never get malware if they got their music legally.

If SOPA and PIPA were passed, the power to protect copyrights would only be in the hands of the corporations even though corporations were offenders of piracy themselves. On December 21, 2011, TorrentFreak.com published "RIAA: Someone Else Is Pirating Through Our IP Addresses" by Ernesto. This article says that the RIAA's (Recording Industry Association of America) own property was being used to pirate copyrighted material. The RIAA claimed it was not them, so they should not be held accountable for their IP addresses' actions, yet they sued thousands of people based only on an IP address.

Corporations also throttle connections to control your personal devices. ISPs always throttled connections even before BitTorrent came out. Throttling connections just because some use them illegally is the equivalent of killing an entire block of people just because some were criminals. It's another position of control. Some, like R. Toby Richards, bend down, take the pain, and accept that's how life is. Others fight back for their rights, like the SOPA, PIPA, and Occupy Wall Street protesters.

Digital piracy is not stealing. It is copying. Believing one less copy would result in one more sale is misinformed. Sales cannot come from those who do not buy anything, whether if it is available for free or not. The opposite is also true: one copy does not also mean one sale loss. On July 21, 2011, *PCWorld* published "Study Casts Pirate Site Users in Good Light" by Ed Oswald. A study conducted by GfK Group found people who pirate movies, on average, buy more media content than those who do not pirate movies. On January 22, 2010, TorrentFreak published "Pirates Are The Music Industry's Most

Valuable Customers" by Ernesto, which states that music pirates are more likely to pay for music and subscriptions. This also explains why profits from the movie and music industries are at an all time high.

By the numbers, if corporations stop piracy, they lose money. Again, copyright laws were never about copyrighted materials or money. It's all a cover for more power. Censoring the Internet would stop the flow of open information and would help these corporations in pushing propaganda. Stopping Megaupload's Megabox or slowing down torrents, which have their own legal uses, allows them to control their industry.

If piracy stopped tomorrow, the government, bribed by corporations, would not give power back to the people. Look at the airports. There has not been another occurrence of hijacking an airplane since September 11, 2001. Osama bin Laden is reportedly dead. Troops in Iraq and Afghanistan are being pulled out. Yet we still have to go through Rapiscan machines and be patted down in the airports. The government, bribed by Rapiscan, is using our tax dollars to treat us like criminals.

"The Piracy Situation" (28:4) does not make sense. If it does, I suggest you take a step back and reeducate yourself on the topic. Piracy allows fans to try before they buy. Malware comes from everywhere, not just piracy. Piracy is right, power hungry corporations are wrong. I hope one day we can return to a world not run by corporations, where someone's daughter is not legally molested at the airport. While the girl cries, their parent, with a defeated look on their face, tells them, "Don't cry. This is what needs to be done. The corporations and the government are right."

Blue Ghost

Advice

Dear *2600:*

I want to respond to Tim's letter in your 28:4 issue. Tim doesn't understand why folks don't want to hire a 14-year-old security expert.

Tim: I was once like you. You have certainly heard before that young men and women your age think they know everything. In hindsight, there's more truth to that than any teenager or young adult can understand. You are showing outstanding potential, but screwing around with vulnerability testing tools and reading *2600* doesn't make you a security expert.

I bet that you could do a fantastic job of helping families to secure their home networks. Turning up WPA2, installing antivirus software, educating folks not to download suspect files, subscribing to Carbonite or some other online-backup service, and I even bet you could build a Dansguardian content filter to keep the kids safe (if not, then I bet you could install and configure commercial parental control software).

Network security beyond that - even for a small business - is something that I wouldn't hire me for when I was young and overconfident like you. There's just too much that can only be learned by experience and formal education. To emphasize my point, I'm going to intentionally refrain from explaining any acronyms (you'll have to Google them). Do you know why VTP can wreak havoc on networks, and how to prevent the problem? Do you know how to rewrite custom programs to avoid SQL injection vulnerabilities? Can you disable telnet on a Cisco device? Have you ever installed a HIPS? Have you ever run SNORT as an IDS/IPS? Can you configure an SSH server to require a certificate in addition to a password? Have you ever run your own Squid server at home to bypass content filters at school (not that I'm advocating such a thing)? Do you know the pros and cons of an RFC 2549 type network?

I'm not writing to burst your bubble. I want to instead suggest that you focus on your strengths. Target the audience that will hire you. If you can secure the home networks of a few friends and family members, then you can approach more folks with your list of references. Be sure not to overcharge. Nobody's going to pay you the same rate as the Geek Squad (although you're probably more skilled than any of those bozos). Personally, if I couldn't secure my own home network, I'd pay a teenager about $10 an hour to do it.

Keep your chin up. Keep hacking. Keep learning. Keep reading *2600*.

R. Toby Richards

Dear *2600:*

If you have found a security hole, and you are not sure how and when to disclose it or are afraid of repercussions from the company which is responsible for the hole, you can always contact the CCC in Germany. They are known for acting responsibly, and they do have legal resources in case someone should threaten to sue them. Unfortunately, their contact info is only in German, but for general requests it's mail@ccc.de. If you prefer to talk to a voice-mail system, it's +49 700 CHAOSFON or +49 40 401801-4300. Point 1 is "Hacker Ethics," Point 2 is "General Requests." Fax is +49 40 401801-40. In case you don't want to overload the "central" point, you can also talk to a local Erfahrungsaustauschkreis. A list of them is found here: http://www.ccc.de/de/club/erfas. In any case, you are likely to find someone who can speak English at a sufficient level.

I'd also like to raise awareness of an issue concerning how *2600* deals with journalists. Di-

recting them to a *2600* meeting certainly sounds like a good idea, however that's not always an option. Often journalists don't have the time to wait for the next meeting, or are unable to attend one. For this, the CCC has special mailing lists with people who are good at talking to the press. If you make it easy for people to listen to you, you are more likely to be heard. Now this obviously would be hard for *2600*. You just don't have the staff to deal with press requests. However, there might be an easier way. Sometimes journalists don't want a comprehensive "official" statement, but the opinion of the "common man" on the street. How about setting up a mailing list to which hackers could subscribe to, and journalists would send their requests, too? This list would be "advertised" to journalists as a way to shout out to some hackers, warning them that since everyone can subscribe, there may be idiots and morons out there. When they write to it, they will be greeted by an auto-reply mail, stating again what this list is and that all replies (which would be sent directly to the journalist) in no way are statements from *2600*, but random voices from the "street." I believe, even though this obviously has issues, it may be a valuable addition to get some hacker viewpoints across, and to make them realize that we are a part of the community at large.

Casandro

It sounds a whole lot like Usenet or IRC. Open communication is a great thing but it should never be confused with intelligent communication. Intelligence can certainly exist within such a forum, but if you offer an equal voice to anyone willing to post, you will get a very low level of it as a rule. We do try and answer or guide journalists who aren't simply looking for a sensationalist headline but we agree that this process can certainly be improved.

Dear *2600:*

I want to start this letter by thanking you guys for publishing a magazine that's informative and interesting year after year. I'm 17, and, as you can imagine since I'm writing to you, am passionate about hacking. I am writing to you because I decided to explore how my passion could be directed towards a more productive medium such as ethical hacking as a career. Since college is looming on the horizon, I have been considering an occupation as a network security consultant and I wanted to know your opinion on whether or not this career path is worth following, as well as other career choices that might utilize my interest and any other tips you might have for me.

Bork

It's utterly impossible for us to advise you on such an important issue without knowing you as a person and having familiarity with your strengths, weaknesses, and interests. You probably know yourself fairly well and even you don't know the answer! Consider this a good thing. It means you have some exploring and experimenting to do. That's what college is for. Use that gathering of the minds to take courses in as many fields as you have an interest in, then ask yourself what direction you feel like heading in after you've explored them some more. People will tell you this isn't practical and that you're wasting valuable time. For them (and maybe even for you - remember, we don't know anything about you), that may be true. But if you're unsure of the direction you want to go, you need to be the one in control and working to follow a path that's unique to you, not just the same as others. Good luck and enjoy the ride.

Dear *2600:*

On page 36 of issue 29:1, you published a letter from an author by the name of "Christian." He was writing in to let you know that he was interested in starting a meeting in Clearwater, Florida. I am interested in starting one as well, and would like to collaborate with him on this matter, as well as a possible hackerspace in the future. Please either forward this email to him, or feel free to send him my email address. If you would like to print this letter (maybe it will catch the attention of some others in the area), please remove my contact information. Thanks!

Mu

We're not a message service, so you'll have to settle for us printing this in the hopes that more people in your area will see it. The best way to approach this is to simply start a meeting and publicize it locally. Once it's been going for a few months and you've sent us regular updates, we'll add it to the official list. Many successful meetings start with only one or two people who are dedicated to keeping them going and who eventually draw a lot more people due to their perseverance.

Social Engineering

Dear *2600:*

I know social engineering and stories thereof are nothing new to the hacking community, but I thought that you might get a laugh out of the time that I accidentally social engineered my own Social Security Number out of my state government.

As a result of scoring well on some Scantron or another in high school, I was awarded a scholarship from the state. I thought I'd used it while I got my AS straight after high school, but a few

years later I got a letter saying that if I didn't use it soon, it would be forfeited. I tried to withdraw it to help continue my education, but it turns out I had miswritten my Social Security Number when I first claimed it, and the paperwork to fix that requires the old info as part of transferring it to the new info.

I called the proper phone number, and gave the brief rundown to the person on the other end. "My name is Forename Surname, I got some scholarship money, when I filled out the papers the first time I had made a mistake on my social - I got part of the SSN mixed up with my high school sweetheart's phone number. I need to know how I'd written it so that I can fill out the forms to correct it." The kind individual on the other end read the digits off to me, no verification needed.

At the time, I thought it was funny that I had "hacked" and "stolen" my own info from the state. A few months later, after reading Rob's article "How to Social Engineer Your Local Bank" in 28:4, I realized just how frightening this was. I could have gotten anyone's info. Anyone could have gotten mine. Fortunately, they would have gotten the *wrong* SSN, but the fact remains that the state forked it over without so much as a second thought. They may have thought it was safe because I said it was wrong, but one could say that about anybody and get their *correct* information, in theory.

At any rate, since it had a happy ending after all, I can safely (if nervously) laugh about it, and I figured that you and your readers might be able to use a laugh (and a heads up).

blanuxas

As with any good social engineering caper, it's all about the story you tell the people on the other end of the phone. In your case, it won the person over and they bypassed their normal suspicions in order to help out.

A Little Feedback

Dear *2600:*

I really enjoyed Cliff's article "Perfect Encryption - Old Style" in 28:4. This was a great simple intro into encryption that explains the basics very well. I had fun creating encrypted messages while away from a PC using only pen and paper. His article created a spark of fun and simplicity. The enjoyment of tinkering with my messages while others looked on gave opportunity to share. Sometimes reevaluating the basics can help solidify my knowledge and show an easier way to explain things to others. Thanks, Cliff, for bringing some fun creativity back.

John Lundin

Dear *2600:*

Has *2600* ever considered opening a fiction section? I'm a semi-pro author and I have a story that'd be perfect for a venue like this.

M

Yes, we've published fiction on and off for a few years now and it seems to be a popular feature. We limit it to one piece per issue and it's always in the very back and clearly labeled to avoid confusion with reality. Please send your submission to articles@2600.com.

Dear *2600:*

Whenever I see a new issue of *2600* in my local Barnes and Noble (oddly, there is usually only one left), I buy it for my fiance (i.e., computer engineer genius man). I surprise him by leaving it next to his "reading chair" in the bathroom.

But not before I read the letters section. I don't understand a darn thing in any of your articles, but the letters and your responses are hilarious, and there are always so many! So maybe I am really just buying your publication for me, just for the letters.

Melissa

The letters continue to be our most popular feature. And now your letter that refers to the letters has made it into the letters. Incredible, ain't it?

Dear *2600:*

I recently picked up my 14-day trial subscription to *2600;* as a programmer just about to graduate and enter network security full time, this magazine looked like exactly the sort of thing that would interest me. I was enjoying the issue a lot and had pretty much made up my mind to keep my subscription when I was taken aback by some gratuitous xenophobia in an article titled "Abuse Reports Still Work." On the issue of takedown notices and the issue of dealing with ISPs in places where English isn't commonly spoken, readers are advised to call the ISP even if they are in "some smelly country."

The author seems to be implying that any country that doesn't speak English is "smelly," an oddly archaic opinion in a magazine that purports to support a modern mindset. Bigotry is not something I am looking for in a programming magazine, and I strongly believe that it reflects poorly on the magazine as a whole.

I hope that my opinions are taken into account for future issues of the Quarterly.

Feroz Salam

We certainly agree that this could easily be seen as an offensive statement, but we also felt there was a chance this was meant in a more sarcastic tone since the concept was so farfetched. That was our hope, anyway. If your interpreta-

tion is correct, then we're comfortable having it pointed out here, accepting the blame, and hopefully getting people to think about such things a little more.

Dear *2600:*

I was reading in 29:1 where Rob T Firefly mentioned that the periods in your Google email/username are optional. There is another extremely useful character Google lets you use: the plus sign. You can use + to "tag" your email so you know where and who it comes from. This makes it easy to track who sells your email and also filter emails from certain people/companies. It works like this: if I was signing up for, say, Groupon, I would use john+groupon@gmail.com. The plus sign and everything after it are ignored and it will arrive at john@gmail.com's inbox, but with the TO: field still saying john+groupon@gmail.com, thus allowing you to track where the email address was discovered.

Scone

Dear *2600:*

Re: "Free Music: The Quest for the MP3" in 29:1 - this was a great article. I myself have been doing this for years. I just have a couple of points to raise.

1. You don't need to use Audacity for this. With YouTube and something like the FlashGot extension for Firefox, or some clever looking-about using the "View Page Source" button, you can download the video by simply inserting that URL ending with .flv or .swf into your browser. If you just want the music, you can then strip it down using Audacity or any free website online.

2. Why did you have to go and spoil the fun for all of us! It was great being the one person out of all my friends who knew how to do this. Not to mention the RIAA is going to buy out YouTube and sue everyone who visits it now. Wonderful.

This article is great at showing that you can't put something onto the Internet without it becoming someone else's. Personally, if information is being broadcast to my machine from any source, that information should become my property if I want.

Valkuma Valkuma

Dear *2600:*

Re: 28:4, page 8 ("Free Phone Numbers with Google"), "and payphones sit unused and broken on street corners...." Incorrect. They aren't broken; they were vandalized. That y'all don't know the difference explains why your political ideas will end up in the trash can of dusty history books.

Re page 5 ("Movements"), one recalls an old saying: "Those who imagine they are running the country read the *Washington Post;* those who think they deserve to run the country read the *New York Times;* those who *do* run the country read the *Wall Street Journal*. I beg to add, those who wear Guy Fawkes masks will end up causing as much permanent change as Guy Fawkes did: zero. Live feeds of Occupy? They are as important as are live feeds of soap operas. So who cares whether the news arrived on an iPod or whether it arrived by Morse code? Well, the same people who pay attention to the *New York Times*.

Lifetime Subscriber

A vandalized payphone is still a broken payphone, so we're not sure why that distinction needs to be made, nor what it has to do with political ideas. As for how much permanent change Guy Fawkes is responsible for, we doubt he'd care but the fact is his name has been printed quite a bit in all of the publications you reference, which must mean something. But change can never be traced back to a single source - it's a constantly mutating process and one that we all have some degree of power over, depending on what we say and what we do. Why would anyone want to believe otherwise?

More Kindle Fun

Dear *2600:*

I have been reading your magazine since I was a teenager - that was a long time ago. I bought a Kindle Fire today and subscribed to your magazine. I noticed one minor flaw. My bank account was not immediately authorized for the funds. I also noticed Amazon accepts any credit card number to store on file as long as it passes the standard Luhn Mod-10 algorithm check. I updated my Amazon account with a very simple Visa credit card number that passes this algorithm check. I used 4111111111111111 Exp: 1212. I realized that every magazine I subscribed to has a trial period. I could subscribe to many magazines with valid credit card info month after month and cancel the subscription prior to billing, but why bother? I just use any old credit card number that passes a Luhn Mod-10 check. Of course, when you bill me, it will be declined so I will just subscribe again and receive another month free, every month. I will actually subscribe and pay for your magazine because I am a devoted old school fan but this is just too easy. My suggestion is that you have the funds authorized immediately and capture the funds once the trial period expires - if Amazon's completely flawed system allows this.

Immune

We have no say over how Amazon does things, but we hope this proves to be a wake-up call for them. It's quite likely, however, that your account would get flagged if you continually did things

like this. You also wouldn't get to keep those trial issues that you obtained through their service. But these are the kinds of tests people should be running on any new system. Thanks for sharing the results and for supporting what we do.

Dear *2600:*

I notice that I can buy individual issues on my Nook, but I can't subscribe through it. I suspect this has something to do with Amazon's Kindle policies (lowest price, etc.), but maybe I'm wrong. What gives?

Erik Marshall

That was indeed the reason at first, but recently we've been trying to work with Barnes and Noble to get our magazine onto the Nook as a subscription. We don't know if it's because they only deal with the big magazine publishers or if they just don't like our content, but we have been unable to get any sort of response from them. We intend to continue trying as we have no reason to keep our content out of people's hands.

Article Issues

Dear *2600:*

I've written articles for *2600* in the distant past, and I'm interested in getting more involved again. One piece I want to query you about is an article about the California Extreme Classic Arcade Show. This is two days of retro-gaming madness held in Santa Clara, California, when private collectors bring out their toys and let everyone play with them. It is enormously fun, with electromechanical games dating back to the 50s, early-era arcade machines like *Space War, Computer Space,* and *Pong,* tons of classics, and even some prototype machines that were never released to production.

So my questions are: Are you interested in such a piece? What is your production schedule and is there any chance that this could make it onto stands before this year's event on July 28-29? What word count do you want?

Thanks!

Phil

If there's a hacking element to all of this, then it makes sense to write something about it. If it's just a review of the show without this, it probably wouldn't fit here. But your letter makes it important to point out a few things. First, we encourage unsolicited pieces. That means you don't have to write and ask if we're interested in something. Generally we are, and, in all cases, we'll at least consider your piece. As we are way too busy to respond to each and every question, this is really the only way we can do this. Our production schedule isn't something you need to work around. We're always putting together an issue and the odds of your piece appearing in one of them increase dramatically once you send it in. As you can see, by the time we got around to replying to your question (personal replies just aren't possible), it was past the date that would have worked for you (although we are able to let people know about the event through this letter). It's always best to simply send in your article. If we don't use it, you've already written it and can send it someplace else or put it up on a website. As for word count, that's entirely up to you. Generally, articles range from 500 words to 3000, but exceptions are always being made. The important thing is to not be too brief and not be too long-winded, and to always work in the hacker angle. With those parameters, it's possible to write on a huge amount of topics.

Dear *2600:*

Do you publish a GPG key or accept encrypted article submissions in any other way? Also, is there a word limit? I have a submission around 1500 words and I'm wondering if it's too long.

Brian

1500 words is a great length for an article. We no longer give out our keys because so many people have yet to master the art of encryption and we wind up spending a great deal of time going back and forth to get a readable copy of something that's meant to be read publicly anyway. Everything from outdated keys to incompatible versions to corrupt files are par for the course. Clearly, we have to have better means of communicating securely over all platforms, but we're not there yet and we just don't have the time or patience to work out all the kinks. We sure hope somebody does.

Dear *2600:*

Why do you keep trying to rob us *2600* authors??? Last I wrote, I got a year of back issues, *and* two t-shirts or a sweatshirt! Now it's only a t-shirt *or* back issues? WTF? In the hopes that you have made a clerical error and are not getting cheaper and more thoughtless to your authors, I would like the back issues from 2011 *and* an XL sweatshirt. If you did change the already slight payment for articles and published the change, I did not see where. I mean, come on! I write for *2600* because I love it and all, but it would not be too hard to use the same material I send to you to other pubs for actual pay and resume fodder. Please don't take away the meager swag that I depend on so much.

If you have, in fact, cheapened up yet again, I would still like the back issues. Please let me know what's up and *please please* consider giving writers back their much needed swag! Good authors are hard enough to find and my payment swag really does help inspire me to write.

Name Withheld

First off, while this communication was sent to our editorial department, we don't believe it was intended for publication. So we've taken pains to eliminate any identifying information. We felt we should make this public so the issue can be addressed loudly, rather than muttered about in private.

We feel compelled to suggest for starters that you get the giant chip removed from your shoulder before it becomes permanent. How someone can be this bitter and claim to enjoy writing for the magazine is hard to imagine. It's just not possible to engage in a constructive dialogue with this kind of attitude.

That said, we're quite aware of the changes that we were forced to make over the years. Many things are behind such decisions and it's never about screwing people over or exploiting them. It's about what we can afford, what's available, the amount of articles in an issue, etc. In the last decade, the amount of articles we print in a single issue has gone up by nearly a third. As with all printed publications, our distribution has gone down, yet miraculously our printing costs have gone up. Despite all of this, the prices we charge, both newsstand and subscription, have remained relatively stable over the years. (In fact, it costs only $3 more for an annual subscription today than it did in the early 1990s when we had 20 less pages!) We also have no advertising income of any sort, nor do we want any. All of this factors in to what we can afford to offer to writers. In the past we've offered less. Then we were able to offer a little more. Now it's gone down to where it was earlier. How things fare in the future will determine what we can do. But if you're primarily motivated to write because you want a t-shirt, you're really involved for the wrong reason. This has always been about getting the word out about things we're impassioned about. The fact that we've been able to do this since 1984 and keep afloat is nothing short of miraculous and a testament to the support network of the hacker community, not to mention the allure of having our own magazine. The fact that we're a printed publication adds to the expense significantly, but it also adds to the longevity in that uniquely analog style. We wouldn't have it any other way.

If you really think we're just interested in screwing people over, there's nothing we can say or do to make you lose that suspicion. We've seen what many other publications offer for non-staff writers and it's really not much, if anything. In fact, most of the material we print wouldn't even be considered by magazines worried about their bottom line or advertiser reaction. If you're more comfortable working with them, then that's what you should do. (We're not sure why you wouldn't want to list us in a resume, however.)

To everyone else, we will always give back as much as we can in as many ways as we can, whether that means t-shirts for article writers, keeping the price of the magazine down, having low-cost conferences with high-price content, donating to causes and institutions that are helping the community, etc. We ask that you help us stay relevant and interesting by speaking up and showing the world what hackers are really all about.

Dear *2600*:

I would like to submit the following article for publication in *2600*. It was previously published in *The New York Times*, but the *Times* informs me in writing that I retained author's rights to republish this piece if I wish. I would be proud to have this article published in *2600*.

Michael

It's a good article, but it's already been published and that wouldn't really be fair to our readers. Our policy is to only print material that hasn't appeared in other places, including magazines, newspapers, and websites.

Dear *2600*:

Thanks to California Paralegal for the info on adverse possession in response to my article in 28:4. I always assumed it was a more complex process and therefore "couldn't happen to me," but no amount of protestation changed what happened at the time. I suspect a lot of quasi-legal things happen "in the dark" and many cases go unnoticed. It's how I also lost the child support I so desperately needed in the 1970s, too. When it stopped coming in, I discovered the court order had been vacated somehow, but I couldn't afford legal help to get it back. I just had to visit the kids on weekends at the babysitter's while I worked two and three jobs. (No, women don't always "get the house." He had a conniving lawyer and I didn't.) Sneaky stuff happens. Just try keeping track of Congress! And that was the real point of my article: watch your back (if you can).

PTKitty

Opportunity

Dear *2600*:

I'd like to add you to my professional network on LinkedIn.

Steven

How exotic.

Dear *2600*:

Thank you for your continuous effort of being a "voice" for hackers out there.

Let me introduce myself. (That looks like a Nigerian scam template, but it's not.) I am the owner of a large security forum. We have over

20,000 members and you can find 600 plus online anytime during the day. I'm interested in advertising *2600* to our members and selling books/items to them. I am also interested in working as an affiliate for your products from our site for a bulk price.

I'd also like to hear more about putting some free articles from *2600* on our front page. We can also put banners to the front page, etc. Articles can be randomly selected by you from old issues.

We never advertised anything yet but I am open to new opportunities as long as it makes some money and educates script kiddies and increases forum quality.

Waiting for a reply at least.

RL

We're going to pass on this. Literally for decades, people have been trying to get us to go this route. It's just not our style. We're not into targeted marketing, demographics, ad banners, or any of that commercial crap that everyone else seems to be doing. We're here to provide information and, as you say, a voice. We don't want to betray that by seeing our readers and contributors as little more than sources of income. Obviously, we need support in order to survive. But we want that support to be tied directly to the work we do, not to our skills in exploiting a market. We're not condemning what you're trying to do and wish you luck in that, but this is just not how we operate.

Dear *2600:*

This is a reminder that on March 25, Steven Leath sent you an invitation to become part of their professional network at LinkedIn.

Accept Steven Leath's Invitation

OK, we can't help but notice that this isn't really a personal invitation, but rather an insidious piece of spam that these people at LinkedIn seem to delight in sending out to everyone on the planet. We're open to suggestion on how to convince them to change their ways.

Observations

Dear *2600:*

In the article "Homeland Security Manual Lists Government Key Words For Monitoring Social Media, News" from the *Huffington Post*, there is a link to the list of keywords that they search for as possible terrorist activity. Under the "Cyber Security" section, "2600" is listed as the top item.

Just thought you guys would like to know that the government considers you a threat. Congratulations on the accomplishment. I look forward to continue reading your magazine even as a government employee myself.

J. C.

That was an awfully odd list, which also included keywords such as "exercise," "facility," "wave," "airport," "smart," "San Diego," "snow," and "social media," not to mention the name of government agencies. We're always happy to be added to lists, especially since in an alphabetical one, we're almost always right on top.

Dear *2600:*

You folks will surely be proud as *2600* made the watch list! (Actually, it *is* sad you're perceived as a threat.) Anyhow, there are now some shirts commemorating these 372 words that are being tracked, and you guys are on it as well! It's item 8592178 on cafepress.com.

Mike
Cape Coral, FL

This is truly the big time.

Dear *2600:*

It currently says on the home page of the Burj Khalifa, the tallest building in the world: "Burj Khalifa features online home-automation and account management access with e-Home and e-Services. (...) With e-Home smart home technology, Burj Khalifa residents can access a totally automated environment for home lighting, temperature, security, access, and more. Coming Soon."

Did they just promise remote access to lights, cameras, and action? I think they did. I guess it remains to be seen if the Dubaians have all their ducks in a row before they do this.

Brother Mouzone

Dear *2600:*

So I saw on 2600.net that you guys have a Twitter. Now I don't really use Twitter, but I thought that might mean you have a Facebook. Well, as it turns out, you do. However, I seriously doubt it is run by you guys since it has such insightful posts as "please send a link for downloading virus source code." Just thought I should let you know.

Patrick

We do have a Twitter, a Facebook, a MySpace, and a Google. We used to have a Yahoo but we lost it.

Dear *2600:*

Are you guys trying to pull a fast one on me? For some weird reason, I was looking at your ISBN information in 29:1, but you all had a typo stating it was actually volume 9! It's not funny.

John Schmitt

We really didn't think anyone even looked at that page. We definitely didn't think anyone could ever get upset at anything that was printed there. Now we know better.

Dear *2600:*

I wanted to submit a photo in case you wanted to print it. Netflix recommended the Nazis' *Triumph of the Will*. And, as I always follow Netflix recommendations, I decided to watch this. Three minutes and 49 seconds into it, I see a plane with the serial number D-2600... no doubt they are smuggling cases of Club Mate.

Eric Botticelli

We've actually heard a lot about plane D-2600 over the years. It happened to be Adolf Hitler's primary aircraft. We really didn't see that one coming when we named the magazine.

Dear *2600:*

Hopefully this is a non-issue, but I felt obligated to tell someone.

I was watching some of the old Beyond HOPE talks, and saw this one. It starts out with someone introducing the speaker (Red Balaclava), and asking that if anyone is going to share video that they please obscure the face and voice of the speaker. Then the speaker gets up... and isn't obscured at all.

I doubt it's an issue (this is a 15-year-old video, after all), but thought someone should know.

Mr. Glass

Thanks for pointing this out. The request wasn't intended for the archives, but for journalists covering the conference on that day. Incidentally, we now have video for our first few conferences viewable online at store.2600.com. Better quality versions are available from us on DVD. Unfortunately, not a lot of people are opting for that, even though we're getting a ton of people watching the videos. This affects the speed and enthusiasm with which we tackle getting the rest of our conferences online - it's a massive job and doing it right takes resources, so we hope people support these efforts.

Dear *2600:*

On your link, http://www.2600.com/phones/newindex.khtml?region=asia, you list Taiwan as a province of China and I am kindly asking you to please, at the very least, replace the current language to Republic of China, Taiwan. This is because Taiwan is not a province of China. China would like to think Taiwan belongs to China, but the reality is that China doesn't own Taiwan.

Ron

Here we go again. We had this exact problem years ago. Our payphone section simply repeats the names of countries as they are listed by the International Organization for Standardization in ISO 3166-1, which is generally seen as an authoritative source. They address this particular issue as follows: "Since Taiwan is not a UN member it does not figure in the UN bulletin on country names. The printed edition of the publication Country and region codes for statistical use gives the name we use in ISO 3166-1. By adhering to UN sources the ISO 3166/MA stays politically neutral." In 2007, the Republic of China, or Taiwan, or Formosa, or whatever, filed a lawsuit against the ISO before a Swiss civil court, saying that their use of the UN name rather than "Republic of China (Taiwan)" violated Taiwan's name rights. It took three years for the case to be decided, but they eventually lost that suit as it was judged to be presenting a political question not subject to Swiss civil jurisdiction. The whole thing is a big mess and we try to stay out of conflicts where tanks and nuclear weapons could come into play. For now, we'll stick with the UN as the authoritative source for naming countries, regions, etc., and that is where you should continue to apply pressure if you want to see a change.

Dear *2600:*

What is it? Well, it's theory that information can be free. What does that mean? Well, it means that someday, everyone will have access to *whatever they want*. And why? Because we can't hide shit and we're too damn smart at picking locks. That's right. We'll have full control and I'm not joking around. Why? Because I write fucking true articles for *Wired* and instead they publish "the news." So get with the program, people. We're it. Open it. Unlock it. Show it. Give it. Yeah, women too, OK. There are like three, no four female hackers in the world. No. Wait, there are two out of one million. So get with the program. Free some data today. But don't get caught. We hate having to get people out of jail. Have fun.

Lynn

We clearly came into the wrong theater about an hour after the feature began. But sometimes it's just fun to ride with it.

Dear *2600:*

Hacker's war strategy:

1. Always kill last.
2. Don't forget about the inons (bits).
3. Deliver the recipe.
4. Forget about vengeance.
5. Be forward but not regardless (impersonal).
6. Always hunt.
7. Be proptive (figurative).
8. Corroborate (akin to) with the masses.
9. Perpetrate no one.
10. Always take the president's side.
11. Forget about diplomacy.
12. Work for Russia.
13. Befriend the aborpo (protrients) (killers).
14. Work alone or aside.

Lynn

We're just glad you're on our side. We're also glad you sent this to our email address which no doubt has resulted in double overtime for the various agencies that monitor it and try to figure out just what it is we're all talking about.

Dear *2600:*

As they say in sports radio parlance, "First time Long time."

In 29:1 Robert T Firefly, *if* that is the author's "True name," writes of a Gmail hack involving one honorable Jebediah Q. Squidfart. A cursory investigation reveals:

jebediahqsquidfart = 18 letters

RichardCheney = 13 letters

Coincidence, my good man? We think not.

Well done, "Firefly."

Myq Morer

And we thought nobody would notice.

Dear *2600:*

I try to listen to your radio show regularly, and find that your group is well informed and up to date. However, I have been surprised that you do not seem aware of the major changes that the new CEO has instituted at Verizon.

They have fewer repair workers. Where they had two men installing FIOS, they now have one, which takes a whole day to install, unlike previously where the two men took three to four hours.

It seems that they are preparing to phase out repairmen without phasing out the practice of billing for the maintenance of the inside wires, the dial tone, and 911, plus all of the various taxes.

If you call 1-800-VERIZON and follow the robot to repair, the robot will run a test on your line and tell you that it will take one minute, and return twice to tell you that the test is still being run. At the end, it will give you the result, and instruct you on how to check the line yourself. This part is unbelievable. It will then ask about an appointment for the repairman to come to your location. When you make the appointment, it will ask you if you want them (Verizon) to call you when the repairman is on his way. They warn you that if you choose to have them text you, you will be charged for the text message.

The dial tone on my phone started giving trouble on February 23rd, on one day, out the other. Since March 4th, there has been no dial tone. I have made two appointments to be at home when the repairman arrives (from 8:00 am to 8:00 pm). To date, no one has showed up. The second time I made the appointment with a human, she said that the repairman said he came and the super said he did not know anyone with my name. I told her the repairman was lying. Later, I asked the super if he spoke with anyone from Verizon and he said no.

There seems to be a battle between Verizon and their staff, each trying to outwit the other in giving as little service as possible and in the middle of this battle is the customer.

It seems that many in government are unaware of Verizon's draconian measures while going into our checking accounts to extract their money without our permission.

I have used phone booths. One number I called was busy, another number just kept ringing. In both cases, I hung up the phone and the money was not returned. Another thing I noticed was that after sundown, the same Verizon number became a different telephone company.

B

We're not really sure what's going on with that last sentence but everything else that you mention is something we've noticed over the years, which seems to have become an unfortunate reality with a number of former Bell companies. We're happy to no longer be their customer on any of our phone lines and we believe many others feel the same way.

Prison Update

Dear *2600:*

Here's a brief update on the criminal case of Jesse McGraw. My email here at Seagoville FCI was unceremoniously revoked last year as prison officials imposed an unlawful disciplinary sanction upon me in absence of any charges or court sanctions that would prohibit me from using email correspondence, violating my First and Fourth Amendment rights. Now I've been in solitary confinement for three months in maximum security for borrowing a friend's email access so I could get info for my lawyer. Since I'm in the midst of appealing my sentence, the SIS Investigation Department is deliberately withholding all of my legal and court documents and new evidence material that would exonerate me of witness intimidation, thus depriving me of my Sixth Amendment due process rights. When I ask SIS why I'm still here, it's always "because of who you are and your charge." (So much for my right for equality!) They've also deprived me of the books I'm writing and denied me access to the media. So, I've notified the American Civil Liberties Union and FBoP regional office. There's no air circulation, the heat and humidity is agonizing which resulted in a death and a few hospitalizations last year with temperatures reaching 115 degrees Fahrenheit. I'm beginning a hunger strike. By God, my spirit shall not be broken, nor will I buckle under the pressure of these injustices. I will win this case. "I am a foe to tyrants, and my country's friend." - Julius Caesar, Act V, Scene 4.

Ghost Exodus

Say It Ain't So Verizon

By Pipefish
email@pipefish.me

You can reset the router password of most stock setups of Verizon's FiOS Internet service without authorization, and without physical access. That is a bold statement, but one that I have found to be true every single time I test it out. And if I've found this out, chances are good that plenty of others have as well. I have called and emailed Verizon several times about this issue and have gotten a mix of "I didn't know that was possible" to "Yeah, that's a value add feature for our customers." Either way, the big V has not addressed the problem. My hope is that if this article gets published in this fine tome that someone brings a copy up to the President of Verizon Security Awesomeness or something, and says "Uhh, we may need to rethink this one!"

I found this issue out by accident, after I moved. I had Verizon come out and transfer my FiOS service to my new address. The tech was doing the usual stuff, then said, "Now I have to verify connectivity. Do you have a computer we can use to test it out?" I ambled up and set my laptop in front of him, which was running Ubuntu. The tech instantly stated, "Uh, we don't officially support machines unless they're a Windows PC." I browsed the Internet and was satisfied. He said, "We have to run a program to test connectivity or I don't get credit for the install." The "program" in question was an exe. *Sigh.* OK, fine, so I booted up my Windows 7 VM. He plugged in a thumb drive and fired off some exe. Now, I won't even go into the fact that I would usually *never* let anyone plug in a random thumb drive to my PC and run some exe, but this was a VM and I wanted him to finish, so I held my tongue. The exe launched some apps that looked like they were testing different aspects of my FiOS service. But for all I know, I was being enrolled in a botnet. But that's neither here nor there.

When all the colors on the screen showed green, he said, "Now I'm going to show you about Verizon's In Home Agent." I didn't feel like dealing with it, but he was in full-on canned speech mode. "It lets you diagnose issues, collect log info for support, and do some other neat stuff, like reset the router password." Fine, fine, get out thank you, enjoy your life tech-guy. When he left, I went to login to the router with the password he had left me (Password1). Of course, wireless security was set to what Verizon always sets it to: WEP. I went in, changed to WPA2 PSK, and changed the passphrase. Then I went to change the password, but accidentally closed the window before I did. Shucks... but wait... the In Home Agent screen was up and the option "Change Password" was sitting right there. OK, I'll bite. So I clicked it. It asked for a new password. It *did not* ask for an old one. Hmm. So I typed in a new password. Then I tried to log into the router. My new password worked. Interesting. Well, maybe since the application was running earlier, it cached the first password when I logged into the site... I dunno how, but maybe. So, I rebooted and repeated and changed the password to something new, without being prompted for the old one. Fascinating. I went to my neighbor later and asked if I could test something out. They owe me since I have fixed their computers for free, so they let me tinker. They let me connect to their network (which was WEP) and I ran the In Home Agent. I then proceeded to change their router password without being asked for the original. Yikes.

In my first call to Verizon, I explained how most times that Verizon techs come out for a FiOS move or install, they set Wi-Fi security to WEP. I was told this was because not all customers' computers support WPA/WPA2, and they want to ensure that their customers can use their Wi-Fi. OK, but WEP can be cracked in minutes. There have been dozens of articles published (some in this magazine) on how to do it. It's easy. But, that's not the worst part. If I get onto a network (crack their WEP or am allowed in), all I have to do is run the In Home Agent and I can reset their router password. I don't have to MiTM them, nor find vulns in their PCs to exploit. I can just own them at their gateway. Redirect DNS where I want, set new routes. "Hmm, I'll inform my manager about your concerns." That's all I got in the first call. Several other calls, and several emails later, there has been no update to the In Home Agent.

I did get one tech who said, "Well, I mean you know, if you're on the network, we figure you're allowed to be... so you can reset the password, I guess." OK, but if I crack the WEP I got on without being allowed to be.... *Sigh.* It doesn't get through. Hopefully, having this in *2600* will get them to wake up. Because a concerned customer's harassment apparently can't.

Hacking Climate Change With WeatherLink

by Cap'n Zilog
capnzilog@moshimail.com

WeatherLink is a cloud service maintained by Davis Instruments (http://davisnet.com/) for the benefit of Davis' network of publicly reporting weather monitoring stations. If you already own a weather station like the Davis Vantage Pro 2, you can add your station to the network with the addition of a WeatherlinkIP data logging network dongle which is basically a set-and-forget device. After a few minutes spent establishing your account and tying it to the device's ID, you can view the basic details of your weather station online along with thousands of others at Weatherlink's global reporting map, http://www.weatherlink.com/map.php. WeatherLink can also be used to share your reports with other networks such as the Citizen Weather Observer Program (http://www.wxqa.com/) or GLOBE Science Network (http://globe.gov/).

The problem is that Davis makes it very difficult to actually get your data out of the cloud once it's in. The software provided by the manufacturer for this purpose is an antiquated Win 3-era program simply called WeatherLink that looks like it hasn't been updated in years. In addition, the source of WeatherLink's cloud data is hidden, the binary data records themselves are kept private, and the software makes it difficult to perform a complete data dump from the Net more than once. The last item may merely be a misguided attempt to reduce the burden on Davis' servers by encouraging incremental data retrieval, but it has the effect of blocking user access to their own raw records for performing long-term ad-hoc weather analysis. It should be noted that WeatherLink software users also have the capability to download recent datasets contained within the memory of their WeatherLinkIPs, but this information is mainly of use for near-term reporting purposes.

The true value of the WeatherLink Network is the time-stamped data cache uploaded by every WeatherLink device connected to the Davis server. These records can go back over two years - with a maximum user archive size currently fixed at 10,240 records. This is sufficient to hold 853 days of detailed weather history (about 500K of information) at the slowest two hour reporting rate. Other interval rates such as 1, 5, 10, 15, 30, and 60 minutes are available, but you can't change the logging rate once your account is set up without losing your archived data. For long-term weather tracking, the 60 minute rate works best, as it's the fastest reporting interval to cover a year's span of time without exceeding the archive limit. Exceeding this means dropping the earliest records, so in order to maintain a detailed weather history of your location from year to year and track your area's climate change, you should download your archives annually.

Fortunately, the protocol for downloading your data is a simple task for any web browser. Sniffing packets while performing a web data grab with a fresh copy of Davis' WeatherLink 5.9.3 software revealed two types of database queries available via the HTTP GET protocol, formatted as follows. First, the Query URL, which results in a server response like so:

```
http://weatherlink.com/webdl.php?timestamp=0&user=[username]&pass=
➥[password]&action=headers
"Model=16 Records=525 MaxRecords=10240 ArchiveInt=60 ConsoleVer=
➥Sep 29 2009 VantageTX=0"
```

This header information is mainly for the benefit of providing support for WeatherLink but it confirms a few useful things: 1) the nature of the weather station reporting, 2) the number of records available, 3) the station's logging interval (hourly, in this case) and 4) confirming the Davis maximum record limit. The username and passwords are yours to supply; the history of every WeatherLink station that's ever reported to WeatherLink is downloadable even if its hardware is down or offline.

Next up is the Dump URL, which allows you to download the data itself and (browser willing) save it as a binary file:

```
http://weatherlink.com/webdl.php?timestamp=0&user=[username]&pass=
➥[password]&action=data
```

Note that since Davis has changed the IP address of weatherlink.com once or twice since I've been following this, as long as you stick to the correct server name you should be fine. However, don't confuse this URL with www.weatherlink.com, which maps to a different IP and may not work.

Davis's raw weather data records follow the Rev "B" archive format, which is public and available at http://www.davisnet.com/support/weather/download/VantageSerialProtocol➥Docs_v230.pdf. These 52-byte records contain every field reportable by Davis Weatherlink stations to the server and then some; if your station does not have solar or soil temperature reporting for example, then the unused fields will be left blank (0xFF). What follows is the breakdown of a typical Davis Vantage 2 Plus weather station record with no extra sensors attached.

Example Davis WeatherLink Rev "B" Archive Record Example (52 bytes)

```
88 15 C8 00 04 02 0E 02 03 02 00 00 00 00 D3 75
```

```
00 00 F7 04 C1 02 2B 44 01 05 0A 0A 00 01 00 00
00 2C FF FF FF FF FF FF FF FF 00 FF FF FF FF FF
FF FF FF FF
```

Rev 'B' archive record (little-endian, LSB first)

```
88 15          ;! archive write date: 1588H = 0001010:1100:01000
               ;  (year=10+2000, month=12, day=8)
C8 00          ;! archive write time H=int(x/100),  M=x%100 = 02:00 hrs
04 02          ;! outside temp. 204H = 516 = 51.6' F
0E 02          ;! high out temp. over archive period 20EH = 526 = 52.6' F
03 02          ;! low out temp. over archive period 203H = 515 = 51.5' F
00 00          ;! rainfall clicks (.01' bucket tips over archive period)
00 00          ;! highest rain rate (in bucket tips per hour)
D3 75          ;! barometer 75D3H = 30163 Hg/1000
00 00          ;! solar radiation W/m^2
F7 04          ;! number of wind speed data packets received 4F7H = 1271
C1 02          ;! inside temperature 2C1H = 705 = 70.5'
2B             ;! inside humidity at end of archive period 2BH = 43%
44             ;! outside humidity at end of archive period 44H = 68%
01             ;! avg wind speed (mph)
05             ;! highest wind speed over archive interval(mph)
0A             ;! direction of hi wind speed = SW
               ;  0=N NNE NE ENE E ESE SE SSE
                  ➥ S SSW SW WSW W WNW NW 15=NNW
0A             ;! prevailing wind direction = SW
00             ;! avg UV index / 10
01             ;! ET in/1000
00 00          ;! highest solar rad over archive period (W/m^2)
00             ;! high UV index over archive
period (W/m^2) [divide this by 10]
2C             ;  forecast rule @ end of archive period
FF FF          ;  leaf temperature ('F+90')
FF FF          ;  leaf wetnesses (0-15)
FF FF FF FF    ;  soil temperatures ('F+90')
00             ;  Download Record Type (0x00=Rev 'B')
FF FF          ;  2 extra Humidity values
FF FF FF       ;  3 extra temperatures ('F+90')
FF FF FF FF    ;  4 soil moistures (cb)
```

The comments with exclamation marks represent fields that also appear in the human-readable "Download.txt" files generated by Davis' WeatherLink software. These contain several items computed by WeatherLink for display purposes which are not present in the raw Davis archive records themselves, including:

```
Dew pt, Wind run, Wind chill, Heat index, THW Index,
➥ THSW Index, Solar Energy, UV Dose, Heat D-D, Cool D-D, In Dew,
➥ In Heat, In EMC, In Air Density, Wind TX, ISS Recept, Arc Int
```

"Arc Int" is, of course, the Archive Interval retrieved from performing the Davis header query described earlier. I'm going to close this article with a data structure for parsing your own WeatherLink Network archives. It's a short step from this to writing a program that can, for example, generate tab-delimited Excel files which you can use to plot your weather history in any manner desired. The sky's the limit!

```
typedef struct {
 unsigned short bfDfDay:5, bfDfMonth:4, bfDfYear:7;
 unsigned short uwWriteTime, uwOutTemp, uwHiOutTemp, uwLowOutTemp,
                uwRainClicks, uwHiRainRate, uwBarometer, uwSolarRad,
                uwNWindPackets, uwInTemp;
 unsigned char  ucInHumidity, ucOutHumidity, ucAvgWind, ucHiWind,
                ucHiWindDir, ucWindDir, ucUvi, ucEt;
 unsigned short uwHiSolarRad;
 unsigned char  ucHighUV, ucForecastRule;
 unsigned short uwLeafTemp, uwLeafWets;
 unsigned char  uwSoilTemp[4], uwRecordType, uwXHumidity[2],
uwXTemp[3], uwSoilMoist[4];
} DAVISREVBRECORD;
```

Baofeng UV-3R: The Cheapest Dual-Band Ham Radio HT

by l0cke

I've recently become a bit of a ham. I made the decision to pick up a couple of Baofeng UV-3R 2 watt 2 meter and 70 centimeter hand talkies lightly after reading a few reviews and learning a bit about them on the UV-3R Yahoo group [http://groups.yahoo.com/group➥/UV-3R/].

It's a cool radio with the comparable portable ham radios costing $100+ more. These things sell for $45 to $50 for one on eBay and that's with free shipping. They take about a week or so to arrive here in the states from China and that's more than acceptable.

I know a lot of hacks have been done with radios over time and even some pranks played on fast food employees with various ham equipment. They work great as a transceiver to hit a relatively near repeater or to scan the local frequencies. I live in a large city so police, emergency response, and taxi drivers are usually what I end up picking up while I scan with it. I'm not going to go into the details of the radio so much in this article. My aim is to give you the means to turn this little dual-band HT into a tri-band HT. From 2 meters and 70 centimeters to 2 meters, 70 centimeters and 1.25 meters. And what's better than that? It's accomplished by the laughably easy method of altering a program (.ini) configuration file on the 1.10 version of the UV-3R Windows software that programs the radio via a $10 (or you can make your own - the plans are around the net) USB programming cable. Yes indeed, frequency expansion can be accomplished with five minutes of work without opening up the insides of a piece of very useful electronics for once! I felt compelled to share it with the *2600* crowd because I know many of you would find this interesting and pretty much anyone on any budget with any level of technical skill can pull this hack off.

Some of the information in this article is from posts in the Yahoo UV-3R group, but it's based upon my experience of doing the software mod myself. Without further ado, here's the soft mod. Enjoy!

The Mod

This is a software modification that can open up more frequencies. You may have a slightly different `settings.ini` file if you have a different software version or one made for a different radio. This is the configuration file for the software that programs the radio. I'd suggest saving the frequencies in Chirp from `danplanet.com` and doing the modification, then restoring those frequencies with Chirp. After that, you can read them from the UV-3R software and use that or just continue to use Chirp if you prefer.

This works for the Vero Telecom/MTC (Main Trading Company) UX-V4 radio as well since it's just a rebranded version of the Baofeng UV-3R Mark II. I've read that this works on the Baofeng UV-3R Mark I as well, but I've only tested it on the latest version (the Mark II).

In the `settings.ini` file for the 1.10 version of the UV-3R software you'll see:

```
[ModelInfo]
```

What follows the # is the profile name (commented out).

```
# Profile 1
```

Then you see the data.

```
Freq0=[136-174/400-470]
data0=6013401700400047
```

You'll see Freq0, data0, Freq1, data1, Freq2, data2.

Those are the three profiles, each profile containing Freq* and data*.

Now, the frequency range is easily seen in Freq0 as "[136-174/400-470]".

Modify that to reflect the desired frequency range. You can also do this to set it to only frequencies you need.

```
"[136-140/400-410]"
```

Now, you also have to modify the next line to get it to work. The first line changes the display in the UV-3R programming software only. The data line (for example "data0") has to be modified too.

It's rather simple. It works as follows. Looking at the fields for Profile Yhree, we see this:

```
# Profile 3 Freq2=[144-148/430-450]
data2=4014801400430045
```

Looking at the data field, we see this:

```
data2=4014801400430045
```

When the line is separated, we see this:

```
data2= 4014 8014 0043 0045
```

Taken apart, the line contents is this:

```
M = Mc and K = Kc
L = Low Byte and H = High Byte
data2= MKMM MKMM MKMM MKMM
data2= LLHH LLHH LLHH LLHH
```

If you wanted to set 144.0 Mc, it would translate to 4014. If you wanted to set 570.0 Mc, it would translate to 0057.

Here's an example of a modified `settings.ini` (programming software configuration file). This is from my computer. I removed one profile as well as the profile names/comments and my com port is set to com port 3.

```
[setup]
com=3
searchcom=1
name=0
language=english
[ModelInfo]
Freq0=[115-400/400-529]
data0=5011004000409052
Freq1=[128-260/390-525]
data1=8012002600395052
```

Hi to PsyWar & <3 & XOXOXO to Dave & Emmanuel.

Transmissions

by Dragorn

Starting this article is a bit of an exercise in desperation, as I attempt to write real content using only the on-screen keyboard of a phone, since an inconvenient lightning strike ate most of my home network.

This is on some level fitting. Recently, the resurfacing of a bug I found in Android a year ago has gotten me annoyed at the utterly broken Android update cycle all over again.

I'm a fan of Android in general. It tends to fall into the bucket of "all phones suck, this one sucks less for what I need to do with it." Unfortunately, in some regards, Android falls down completely, especially when it comes to security updates being pushed to older handsets in a timely fashion.

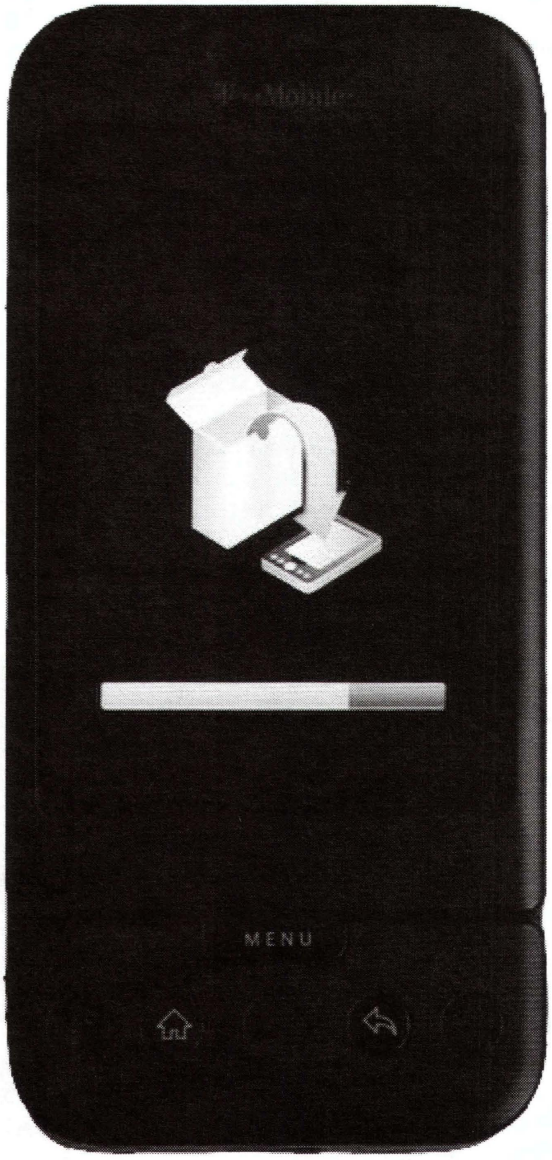
Many factors are at play controlling when updates are pushed to phones, and few of them represent the best interests of the consumer. The side effects of this are probably being felt by many of you right now: How many of you are still waiting for Android 4 to be announced for your device, let alone delivered?

When Google releases a new Android update, it typically first appears as a firmware for Google-sponsored and developed phones (the Nexus series), and sometimes released as non-open-source firmwares for specific vendors (Honeycomb or Android 3.x for example saw binary releases while never seeing an open source release until Android 4 was complete).

Unfortunately, most consumer phones are not directly based on the Google reference design. Attempting to differentiate themselves from each other and provide consumer lock-in on a specific brand, vendors modify the base Android system. Modifications run the gamut from the innocuous (custom widgets and home screen launchers), to the annoying (custom UI layers which can lead to applications looking weird and slow down the system), to the infuriating (enhanced logging daemons with vulnerabilities which subvert the permissions system of Android and allow applications to greatly exceed their declared permissions).

Finally, the carriers get involved, requiring specific features in stock Android to be disabled to allow billing users extra to unlock them (such as hotspot mode), requiring applications be installed (bloatware and crapware apps for which the carrier gets a cut), and often they require that the bootloaders remain locked to prevent users from installing custom firmware which lack these restrictions.

Each layer adds a delay: modifying a system as complex as Android definitely takes time, and validating all those modifications



take even more. Validating that the firmware behaves as expected and won't negatively impact the carrier's network also takes time and money.

Unfortunately, it's not in the vendors' best interest to expend extra effort building new firmware images, testing them in-house, and paying for their testing out-of-house on phones they aren't getting money from. In some cases, the phone simply lacks the RAM or storage space to run a newer version of Android (feature creep, like any OS, usually means every revision is a little hungrier than the last for whatever resources the phone can give it). But often, a manufacturer (or a carrier) decides that a phone is end-of-life and will no longer get updates, even when the device is fully capable. The only recourse for the user? Buy a new phone, truly a horrible outcome for phone manufacturers.

This has serious implications beyond not getting the latest shiny version of Android. Security updates also fall by the wayside when phones no longer get timely updates, and even phones which are slated to get updates may get them months after a security problem is made public, leaving the users exposed.

For example, say a new vulnerability is discovered in the now much older Android 2.2. While any device capable of running 2.2 should have a reasonable expectation of being able to run 2.3 with no problem, Google's own numbers show Android 2.2 at 19 percent of the Android ecosystem, and Android 2.1 (current around 2010) still holds five percent of the installed devices. Looking through anger-tinted glasses, a moderately reasonable interpretation is that 25 percent of the Android devices currently deployed are completely abandoned by their manufacturers and carriers, and any exploit found in them has a very good chance of never being fixed.

A familiar tune to everyone should be the oft-repeated (and oft-ignored) reminder that a smartphone is just another PC, with a permanent Internet connection and links directly to your credit card. It's an extremely tempting target for malware, despite none being terribly advanced so far. Like the Java worm which just hit OSX, Android can remain unscathed from a serious widespread attack for only so long; when vulnerabilities exist, and money can be made, eventually someone will step up to take it on.

For hackers, of course, solutions abound: root your phone, run AOSP or a custom ROM, and you're good to go... mostly. By running an un-vetted ROM image, you are open to attacks against credentials, logins, call snooping, and so on: It's an untrusted operating system, often assembled by unknown (or semi-known) individuals. So far, no custom ROM has gone black-hat (or at least been detected as doing so) and I in no way cast aspersions against any ROM developers, but, the risk remains: by trusting a relatively unknown source, you trust that they never become malicious, and that they are never compromised themselves, exposing the build system used to create the ROMs.

For normal consumers, installing a custom ROM usually isn't an option.... and we should care about this. If you're an Android user, the entire ecosystem of the Android platform is relevant: if the platform degenerates into dead-ended devices which will never see an update, developers will leave, and the developers who remain will be shackled to deprecated versions and unable to take full advantage of newer Android features without sacrificing 25 percent of the market.

It's difficult to influence the course of large corporations who make the phones and carriers who control releases, end-of-life, and bloatware installs, but it behooves all of us to demand reasonable update guarantees whenever the option presents itself.

2651 OLIVE STREET SAINT LOUIS MO 63103

420 SOUTH GRAND LOS ANGELES CA 90071

611 FOLSOM STREET SAN FRANCISCO CA 94107

51 PEACHTREE CENTER NE ATLANTA GA 30303

10 SOUTH CANAL CHICAGO IL 60606

30 E STREET SW WASHINGTON DC 20024

811 10TH AVE NEW YORK NY 10019

12976 HOLLENBERG DR BRIDGETON MO 63044

Metaphasic Denial of Service Attacks

by Everett Vinzant

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network resource unavailable to its intended users. In a denial-of-service attack there is an implied one-to-one relationship between the attacker and the victim. An example of this is using a computer on the Internet to send so much traffic to a server that the server fails to process it all. As this failure occurs, other traffic is left unprocessed. This prevents legitimate users from connecting to a website, processing orders, or accessing email.

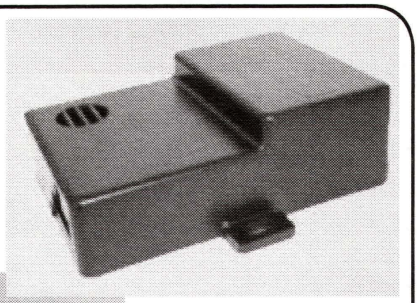
A distributed denial-of-service attack varies only in the structure of the attack. In a distributed denial-of-service attack, there is an implied many-to-one relationship between the attacker(s) and the victim. Typically, an individual or entity (crime family) will commandeer control of hundreds or thousands of computers by a virus or trojan. Once this network of computers is created, they can "gang up" on a server. The end result is the same, the server is overwhelmed, and service fails.

The possibility of a third attack type exists. This hybrid of the two attacks offers a distinct advantage that will be addressed. Metaphasic denial-of-service or MDoS is a method of combining several denial-of-service attack types. Some of the same techniques used in a DDoS attack are employed. First, hundreds or thousands of computers are taken control of. The same method used for DDoS will be effective for this (viruses, trojans, etc.). If there are a thousand computers in the created "zombie net," it is divided into multiple serfdoms.

Each serfdom is assigned a specific DoS attack type. One serfdom may attack TCP/IP handshakes. One may attack an Apache server. One may attack SQL databases. After five or ten serfdoms are created, an attack is initiated with the first serfdom. The attack lasts five to seven minutes. Then the first serfdom's attack ceases, while the second serfdom's attack begins. This process occurs until all serfdoms are exhausted (everyone has had their turn to attack). The length of the attack can easily be an hour.

There are several reasons for this attack. First, it's a matter of psychology. The first attack will be detected, but not responded to in five to seven minutes. By the time this is identified as an attack, it ceases. The assumption exists that someone upstream has identified the problem and stopped it. Then the next attack begins. The attacks occur until all of the serfdoms have fulfilled their role. Second, because this method rotates types of attacks specific to the network being attacked, there is actually an hour of DoS. Third, and most importantly, you have the undivided attention of the security group at a given location.

This is the crucial part of the Metaphasic denial-of-service attack. Since everyone is focused on the DoS attacks, a firewall/IDS bypass attack is used. While the security department is focused on an incoming attack, they miss the surgical strike done to the network. Logs may not be examined. If they are, unusual traffic may be credited to the DoS attack, providing cover. This is a classic distraction/flanking maneuver.



Never be ON TIME Again!

by OMK

The Problem

This spring, I bought a 1997 Subaru Impreza from a friend. I paid cash for it, and was in the process of cleaning it up on a Sunday afternoon when I opened the glove box. Inside was a small plastic device with a green LED, and four buttons numbered 1-4. A cable ran out the back of the box into the dashboard. Curious, I unplugged the device from the cable, and turned it over in my hand. There was a label on the back that read "ON TIME - Payment Protection Systems, Inc." It didn't mean anything to me, so I shrugged, plugged it back in, and the green LED was now red. And my car wouldn't start. Lovely.

Some reading on the Internet confirmed what I suspected. ON TIME is an ignition interrupt. In a nutshell, it disables the vehicle ignition if a borrower fails to make an auto loan payment on time. These types of "payment protection systems" are intended to make it safer for a lender to make high-risk (and high-interest) auto loans. They install an ignition interrupt, program it with a payment schedule and ransom codes, and send the borrower home with a car that they probably can't afford. When the borrower makes a payment, they are supplied with a six-digit ransom code that they punch in to the device, buying them another thirty days. When they fail to make a payment, they don't get the code for that month, and the car no longer starts. Some of these systems also include a GPS, so the repo man can cruise casually out to the location of the now-disabled vehicle, enter the code, and drive it back to the car lot. And probably sell the vehicle again to somebody else who can't afford it.

Of course, such systems fail. In my case, I had purchased the car used, not even knowing that it had an ignition interrupt installed. When the last payment had been made by the original buyer (or when the repo man took the vehicle back), the ON TIME unit had never been removed. The battery in the control unit was apparently dead, so when I disconnected the cable, I essentially reset the unit, and it was awaiting a ransom code input before I was allowed to drive anywhere. I called the girl from whom I had bought the car, and she didn't know anything about it. She had bought the car used from a dealer, and had also paid in full up front. I called the dealer, but they were closed on Sunday. Even if they had been open, they probably couldn't have helped; the paperwork showed that they had received the vehicle as a trade-in. Whoever knew the codes for the ON TIME device had programmed them in 1997, and I wasn't likely to find them, particularly not on a Sunday afternoon. In the meantime, my car was dead in the driveway.

The Solution

So I went back to the ON TIME control device. I pushed a few buttons. They beeped and the LED flashed red again. Brute-forcing combinations by hand wasn't an attractive option. According to the ON TIME website, the codes are six digits long, so there are 4096 possible codes using the numbers 1-4. Not a lot for a computer to guess, but a lot of buttons for me to push. I unplugged the device again. The data cable had eight pins, presumably used to program the device. And then plugged in... to what? I traced the cable behind the dashboard, toward the steering column. Four or five screws later, I had the steering column open. The other end of the data cable terminated at a

relay box with a wiring harness plugged into it. The harness had only four wires going into it, so I traced those. Two of the wires were spliced into existing factory wires. Those presumably provided power to the control unit. The other two were the interesting ones. A section of the vehicle ignition wire was cut out, and the circuit was routed through those two leads in the relay's wiring harness.

From here, it was easy to fix. A circuit has two positions: open or closed. So the ignition circuit routes through the relay box. The relay box receives signals from the control unit with the buttons. If the control unit doesn't receive the ransom code in time, it tells the relay to open the circuit, and the ignition no longer works. So: no reason to mess with the control unit. I disconnected the data cable and threw it into the yard. The control unit went in my shirt pocket. From the relay box, I disconnected the wiring harness, cut the ignition wires from it, and twisted them back together with a wire nut and some electrical tape. Circuit closed. I turned the key to make sure the car started, and then put the steering column back together. And marveled that the stupid thing had been in there for fifteen years.

Lessons Learned

Ultimately, what I did wasn't particularly difficult or clever. I just snipped a couple of wires and twisted them back together. Finding and replacing a bad fuse in my clothes dryer had been more difficult than that. What I found interesting upon reflection was my first instinct: get the codes for the ON TIME control unit. Because that was the interface that I could *see* - the one with which I was *supposed* to interact. And it was entirely the wrong instinct. If I had messed only with pushing buttons on the control unit, I would probably still be trying to brute force guess the ransom codes. As it is, I still have no idea what the codes are. But I don't care, because the control unit is in pieces on my desk. I could have wasted a lot of time trying to read I/O from the data cable, but the problem was easily solved in five minutes by going to the power source with a screwdriver, a set of wire cutters, and some electrical tape.

Find and mess with the parts of things that you aren't supposed to find and mess with, and not just the parts that you can see at first glance. And don't insist on a complex solution when a simple one will do!

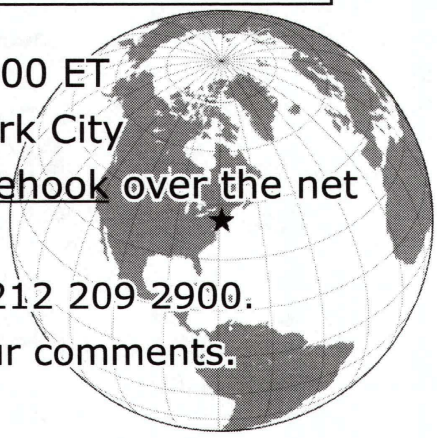
References

- http://ontimedevice.com/

OFF THE HOOK

TECHNOLOGY FROM A HACKER PERSPECTIVE

BROADCAST FOR ALL THE WORLD TO HEAR



Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite.
Contact us if you can help spread "Off The Hook" to more listeners!

by Andy Kaiser

Chapter 0x1

Rain pounded the pavement as I huddled in the doorway. There were no streetlights here. Not in this part of town. Apart from periodic lightning, my phone's display was a rare flash of illumination. The weak blue light shone on my face and lit my eyes like anemic sparklers.

I glanced up at the sky and squinted into the darkness. For early evening it was unusually dark. The black thunderclouds in the sky made sure of that.

I was outside my client's building and was close to my target: A window one story up.

I stepped out from under the roofline and rain attacked my head and shoulders with thousands of tiny punches. I held up my phone and shielded the lens from rain with one hand as I took a sequence of infrared pictures. I fell back under the shelter of the building. I swiped raindrops off the cellphone screen as I zoomed in to examine the results.

Despite my mood, I smiled.

I never liked working in this part of town and I particularly didn't like this client. Despite the weather outside, it was more annoying inside. But I was done. Mission accomplished. Time to go back in and collect my due, if I could.

Warren Relegaard was the client today. He may have been Swedish. Maybe Greenlandian. Or he was just an American who dressed weird and used a fake accent. There were plenty of those around, too.

He sat in a brown, oversized, overstuffed armchair.

Some people looked alike. A husband and wife who lived together and loved each other for fifty years and had the same conversation a hundred times eventually would become mirror images of each other. They used the same muscle sequences to talk and gesture, the same thought processes to communicate, the same glazed expression to stare at the TV night after night. Like perpetuates like.

I'm not saying Warren Relegaard was married to his armchair, but I am saying it had been a significant part of his life for fifty years minimum. It looked like him, all leathery, worn and overstuffed. I smelled pizza rolls. That was usually a pleasant experience, but now it creeped me out because I had no idea where the smell came from. The more I worked with him the less I wanted to work with him. Dislike perpetuates dislike.

"This night, Mr. Manny," he said in his possibly fake accent, "I do not think you have found what you claim."

"Sorry. I did."

Relegaard lifted a single thin eyebrow, which was probably an effort on a face with that much excess flesh. He gestured grandly at me.

I was fluent in non-verbal communication. It was a job requirement for us, the elite players of my profession. But non-verbal was for accidental slips, for finding what people didn't want us to know. I didn't like it when people used it intentionally. It always seemed forced. Arrogant. So I played dumb and continued to stare.

He exhaled a deep sigh, giving me a possible clue as to the origin of the pizza roll smell.

"*Please,*" he overemphasized. "Tell me what you've accomplished."

"I hate to tell you this," I said, loving this part. "But it's true. Your wife's cheating. And it's happening right now."

He said nothing. His face reddened and he began to breathe heavily. Angrily.

That was the kind of non-verbal communication I could work with.

"Now?" he said. "Upstairs?"

"Yes," I said, not feeling particularly bad. I'd seen it plenty of times before.

His face got ugly and he pushed with both arms to lean forward in his chair. "I ask that you prove it, sir."

"Go ahead and log on," I gestured to his tablet sitting on a side table. It was an older model. He grabbed it and turned it on.

"Check the link I just sent you."

He opened an application and waited. He tapped impatiently on his chair.

"This machine. It is so slow. Why is that? How can I make it faster?"

Check for malware. Don't have twenty unnecessary programs running at all times. Pay money to get better hardware.

I shrugged.

He checked his mail. My message redirected him to a private, secure site I used to give information to my clients. He stared at the file list contained there.

"What are these?"

"Open the first one."

He did. Five seconds later he realized what he was looking at. He gasped.

"She's not -"

"She is. Second file."

He opened that one, too. Then the rest. I kept quiet as the photos did all the talking. I watched his face get redder and darker as he saw uncensored, candid pictures of his wife in very compromising situations.

"I see it. But I cannot believe it."

"I'm sorry, Warren. I know you thought better of her, but she's not what you think. She's cheating."

"No!"

"Yes. When you go online to play TekMage with her, she wins every time because she's been using a programmable keyboard meant for online gaming. She cheats. You never found out, because by the time you got upstairs," I imagined his huge frame navigating a stairwell, "she'd have hidden everything. She'd have unplugged the gaming keyboard and swapped it out for a five dollar generic keyboard. After you go back downstairs and keep playing, she's back to cheating."

"That's why she never wanted to play in the same room as me!"

I took shallow breaths in order to avoid the smell of pizza rolls.

"Yeah. Maybe."

The reason I kept coming back to Warren Relegaard was that while he was cheap and annoying and mysteriously odorous, he paid me in cash and seemed willing to hire me again. Though this job had been far more personal than the others. I hoped it hadn't killed our business relationship. I made a mental note to make up an impressive-looking coupon for future services and send it to him later.

"Okay," I said, readying myself for the next phase of our conversation. "I'll leave it to you to get the situation under control. I have the bill. You get the surveillance photos of her using the device, as well as millisecond-stamped, in-game screenshots to prove she couldn't physically type some commands without special gaming hardware. I worked for five hours on this. You know my rates. I'd like -"

"Yes, yes. Now we discuss your payment."

Then he tried to justify why my time wasn't worth what I knew it was.

I'm regularly amazed at the number of people who think it's socially acceptable to regularly haggle with someone who makes their living charging by the hour. It didn't quite convince me to get a normal, dependable salaried job as Information Systems Director at the Corporate Office, but on days like this I gave it a second and third thought.

My name is Dev Manny. I'm an Information Technology Private Investigator. My clients call me when they have technological problems. Some people assume I'll fix their broken printers and upgrade their equipment, and I do: It's easy and routine, part of the occupational churn that pays my bills.

I preferred the exotic cases. I've been pulled in by the police when they got in over their head. I've been hired by corporate CEOs when they needed IT covert assistance without having to alert any of their staff. I had friends in the industry, many of them as good as me or better in information technology. But while many of them actively looked for complexity, mysteries, and problems the way I did, not many addressed the human element.

IT workers need a primary toolset of intelligence, best practices and the ability to find information online. I went outside that zone and focused on people. Their behavior, their personalities, why they behaved the way they did. Throw in fraud, theft, and, yes, sometimes murder, and you needed more mental tools to handle those situations. That's where I came in.

Out of all the people I knew in the industry, no one did what I did. I like to think it was because I was unique, the special little snowflake my mother always told me I could be. I've also had people tell me it was because no one was stupid enough to drop to my pay scale and undependable wages.

Speaking of income, I was indeed in a dry spell. I'd had limited work for too long now, nothing I could label a case. Relegaard's issue might be moderately intriguing, though having to deal with the man himself put this work firmly in the "do not want" category.

I left Relegaard's place shivering and cold from the rain, and also from my wallet's latest addition: A limited number of small bills.

Still, in this case, the exchange of money for information was worth it. I had a new ability compared to just a few minutes ago. A power-up, a financial mod, a new level of achievement which put me in a class of people I rarely got

to join.

I now had the ability to purchase dinner.

Chapter 0x2

I levered myself into my completely untrustworthy 1999 Nissan Sentra and turned the key. After a blast of automotive profanity which I'm sure would fog the mirrors of any nearby cars, my car grumbled out of Relegaard's snakelike driveway and shuddered in fear as I gained the open road.

I had decided long ago that I liked this car. Loved it, in fact. Because the alternative to not having it was to use my feet. My Sentra was like my first high school relationship: Something that had no business being in public and was in desperate need of lubrication.

My car allowed me to get to one of my favorite haunts, a scummy bar called "Downway." I walked in and dropped into a sticky booth in the corner.

A large, thick roll of brown, misshapen carpet walked up to me and bent over the booth.

"Hey, Manny," it rumbled.

After a second glance, I realized the carpet was actually Ron-Don, the judge, jury, and executioner at Downway. More importantly, he was the barkeep. Most importantly, he was the owner.

"How's life, Ron-Don?"

He shrugged. If any normal human tried the same thing with the same amount of weight, their shoulders would snap. He made lifting a metric ton of solid muscle look easy. He'd been some kind of weightlifter years ago, and he still kept in shape. Seemed like a lot of unnecessary work to me, but, on the other hand, no one caused trouble in Downway, at least not more than once. It was one of many reasons I liked coming in here: I could use the free wireless in peace.

"I'm living," his voice rumbled. "You?"

"I won't complain."

"So you got problems then?"

Ron-Don might not look like the most intelligent guy, but you'd be surprised. He didn't miss much.

"Who doesn't?" I said. "I won't bore you. Besides," I pulled out my wallet and flashed him my wad of singles, "I've recently come into some money. I'd like a burger and your finest glass of caffeine."

"Go crazy, man."

Floorboards protested as he left to place my order.

While I waited, I checked my cellphone and flicked through my existing workload. I was done with Relegaard. In the meantime, I was waiting for payment on a few closed cases. Apart from that, I had nothing else in the hopper. I'd have to find more work soon, assuming I still wanted to eat in the daily way I'd been accustomed to.

"He's watching you."

I was so intent on staring at my phone, I didn't notice Ron-Don had returned until he spoke.

I blinked up at him. "What? Who?"

Ron-Don placed a burger and drink on my table and cocked his head to the side.

"Over there," he muttered. "Dude in the other corner. He's by the window."

He was indeed. He was facing away from me at the moment, and was staring out of the dirty, smudged window. His face was in partial shadow, so I couldn't see him well.

I slurped what I assumed was warm coffee and began to eat. Halfway through my burger, I pretended to resume work. I popped open my laptop. I used the screen as cover as I started my cellphone's camera app.

I casually lifted the phone. I pointed it towards where the guy was sitting and pretended to examine and frown at something on the screen while I took a movie.

It was the best I could do on short notice. My actions were probably as transparent as a giggling fanboy who just saw that hot *DS9* actress (and let's be honest - there is only one). But I had to do it - I liked to get things recorded before I did something about them - it was insurance if I needed to get others involved, like the law, or Facebook.

I quickly finished eating. Strange mysterious watcher or no, dinners I could pay for were rare enough that I didn't want this one interrupted.

I snapped my laptop shut and got ready to go. I left a depressing ratio of Relegaard's bills on the table, then I headed over to where the guy had been sitting.

He was gone.

I sighed.

What's wrong with our society? Can't people just talk anymore?

I took out my phone and checked the video I'd just recorded. I brightened the movie, increased the contrast, and zoomed in to get a better view of the guy. I played it back.

Ron-Don was incorrect. He'd used the wrong word. This was no dude. It was a kid. High school at most. He was dressed like he was homeless, which, combined with the nice cellphone and the ear buds stuck in his ears, meant a rich kid with richer parents.

I was only twenty-six. I was too young to be called "old" by most, and could sometimes get away with looking younger. This kid had

the opposite trait. He had something that made him older. It was written in his appearance, not just his limp dark hair and pale skin, but his attitude, punctuated with an oddly-thin body and gaunt stare. This kid was messed up. He'd been through something, and it was big.

I realized what I was doing. Great Old Ones, I was thinking of this kid as the stereotypical antisocial computer nerd. I sensed the ghost of Steve Jobs above me, sadly shaking his head. *Well,* I mentally shrugged back at Steve, *stereotypes are self-perpetuating.* Steve rolled his eyes and disappeared in a puff of cloud computing.

As I watched the video, the kid was working on his phone, just like I'd pretended to do. He pointed his camera at my own.

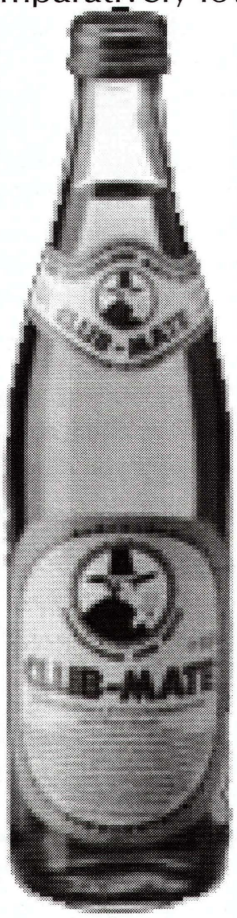
He was taking shots of me, just as I'd done to him.

I revised my earlier theory. The kid hadn't been through something big. He was in the *middle* of something big. And it ended with me.

This is the first in a series of chapters from the newest Dev Manny, Information Technology Private Investigator *story. You can find the first book (*Superliminal*) on Amazon and other places. Please let us know if you want to see more - or if you want us to stop. Write to letters@2600.com.*

CLUB-MATE

Club-Mate is now ready to be shipped directly to you! The German beverage invasion is now in full swing and 2600 is happy to be in the thick of it. Club Mate has proven to be extremely popular in the hacker and programming community. First introduced in the United States at The Last HOPE in 2008, this caffeinated, carbonated, comparatively low in sugar drink has really taken off. Both HOPE attendees and German operatives tell us that one gets a burst of energy similar to all of those energy drinks that are out there without the "energy drink crash" that usually comes when you stop consuming them.



If you want a case of the stuff (12 half-liter glass bottles), it's $55 including shipping. At the moment, we can only ship to the continental United States. Visit our online store (store.2600.com) to place an order or call us (631.751.2600) if you have further questions.

For those of you running an office or a hacker space, consider getting a full pallet (800 half-liter bottles) at a steeply discounted rate. You will have no trouble reselling to the addicts you create.

Further updates on club-mate.us.

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $150 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, email us at happenings@2600.com or by snail mail at Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

July 13-15
HOPE Number Nine
Hotel Pennsylvania
New York, New York
hope.net

July 26-29
Defcon 20
Rio Hotel and Casino
Las Vegas, Nevada
defcon.org

July 26-29
HaxoGreen
Belvedère Campsite
Dudelange, Luxembourg
haxogreen.lu

July 28-29
Maker Faire Detroit
The Henry Ford
Dearborn, Michigan
makerfaire.com

August 8-12
ToorCamp 2012
Hobuck Beach Resort
Neah Bay, Makah Indian Reservation, Washington
toorcamp.org

August 14-18
ETH0
het Boshuis, The Netherlands
eth0.nl

August 31-September 2
Electromagnetic Field
Pineham Park, Milton Keynes, United Kingdom
emfcamp.org

September 27 - 28
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.org

September 28-30
DerbyCon
Hyatt Regency
Louisville, Kentucky
derbycon.com

September 29-30
World Maker Faire New York
New York Hall of Science
Queens, New York
makerfaire.com

October 24-28
ToorCon
San Diego, California
sandiego.toorcon.org

December 27-30
Chaos Communication Congress
Berliner Congress Center
Berlin, Germany
events.ccc.de

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

For Sale

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, poker cheating equipment, computer devices, odometer programmers. and much more. www.hackershomepage.com

OUR MOST POPULAR OPEN SOURCE PROJECT, Bus Pirate is a universal bus interface that talks to microchips from a PC serial terminal. Here's how it works. When either you or your software script enter commands into a terminal on your computer, those commands are interpreted by the Bus Pirate and sent via the proper protocol. The Bus Pirate then interprets data sent back to your computer terminal - and you see the response on your screen. Simple! The Bus Pirate is public domain, you are free to rework and reuse this design in your own projects. $30 including worldwide shipping @ DangerousPrototypes.com.

PRIVACYSCAN FOR MAC OS X seeks and destroys potential online and offline privacy threats with 35-pass wipe. Available on the Mac App Store for a low introductory price - http://privacyscan.securemac.com

CLUB-MATE is now available in the United States. The caffeinated German beverage is a huge hit at any hacker gathering. Now available at a reduced price of $55 per 12 pack of half liter bottles INCLUDING SHIPPING. Bulk discounts for hacker spaces are quite significant. We also have a limited supply of Club-Mate Winter Edition. Write to contact@club-mate.us or order directly from store.2600.com.

BUS PIRATE, our most popular open source project, is a universal bus interface that talks to microchips from a PC serial terminal. Here's how it works. When either you or your software script enter commands into a terminal on your computer, those commands are interpreted by the Bus Pirate and sent via the proper protocol. The Bus Pirate then interprets data sent back to your computer terminal - and you see the response on your screen. Simple! The Bus Pirate is public domain, you are free to rework and reuse this design in your own projects. $30 including worldwide shipping @ DangerousPrototypes.com.

PORTABLE PENETRATOR. Crack WEP, WPA, WPA2 wifi networks. Coupon code for Portable Penetrator Wifi Cracking Suite. Get 20% off with coupon code 2600 at http://shop.secpoint.com/shop/the-portable-penetrator-66c1.html

GRRIPZ, a new bag carrying device developed at Alpha One Labs, a hacker space in Brooklyn, NY are now available in a variety of colors individually or in retail boxes of 10. See Grripz.com. Post online or send us a photo of your sore hand after carrying bags for a chance to win two luxury Grripz :) Twitter @grripz or email info@grripz.com

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

Help Wanted

CAN'T HACK? Won't ddos? You want to help anyway? Help us here! Get active at wiki.freeanons.org and support the Anonymous Solidarity Network!

AUTHOR NEEDS INFORMATION FOR MANUSCRIPT about methods and tactics used to hack voice mail accounts in England and U.S. Will pay cash for verifiable information. cabledescramblerguy(at)yahoo (dot)com

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

NO COMPROMISE PROVIDER of open architecture-based network privacy & security services is actively searching for exceptional technologists (of all hat colors) with extensive experience in network topology/design, VPN architectures, and general *nix sysadmin - we recently survived a massive federal effort to shut us down via extralegal harassment & imprisonment of our founding CTO on political grounds; company is now bouncing back & expanding our service offerings (telecom included). Must have strong loyalty to principles of free expression, anti-censorship, genuine cultural diversity. Tribal-based management philosophy - strong financial performance, strong community involvement. Details, compensation info, & longtime community credentials available via: wrinko@hushmail.com. Namaste.

Wanted

WE'RE ACTIVELY SEEKING SUBMISSIONS for a new print magazine covering a broad range of tech/non-tech subjects, such as: proven physical security techniques, "Breakdown of a Takedown" (dissections of law enforcement attacks), real-life financial privacy tactics, cross-jurisdictional lifestyle tutorials, implementing genuine privacy in the cloud, configuring private smartphones, etc. Geared to non-specialist audiences, 100% non-profit, & community-powered. Be a part of the first issue - share your wisdom! Info: privatelifestyles@hush.com.

Services

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

NOPAYCLASSIFIEDS.COM - Free advertising in 50 countries! Free business directory ads with link to your website to help expand your business and improve search engine placement. Free classified ads! Over 35 million classified ads to help you find what you want by searching over 75,000 different social media and online classified ad websites. Thank you for being part of our online audience.

COMPUTER FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality computer forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Sensei forensic technologists all hold prestigious forensics certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on computer forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even *O* magazine. For more information, call us at 703-359-0700 or e-mail us at sensei@senseient.com.

JEAH.NET UNIX SHELLS & HOSTING. Quad 2.66ghz processors, 9gb of RAM, and TB and TB of storage? JEAH.NET is #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Don't forget our free private WHOIS registration service, with domain purchase, at FYNE.COM.

Announcements

SEND A *2600* GUY TO CONGRESS. www.DaveChapmanForCongress.org I am a *2600* subscriber and will try to reduce the cluelessness level in Washington. If you are in Silicon Valley, vote for Dave Chapman.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2011 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

Personal

INCARCERATED ELITE HAX0R/GAMER LAMER. I am a 40-year-old male hax0r/gamer lamer from the Houston, Texas area. I have been under lock and key since 2005. I am currently seeking pen pals and new friends to help me finish my last 14 months until freedom. I am interested in anything hacking, cracking, phreaking, modding, spoofing, & anonymity. I am especially interested in anything cellular, wireless, or smart phones and anything else that I can add to my arsenal. I have been around since the C-64 days when it was all about BBS's and phreaking Ma Bell. I have missed out on a lot in the past 7 years. I am looking for someone to help me get caught up on everything I have missed. I also enjoy good rock, techno music, & good beer. You can send me an email by going to www.jpay.com & using my info or you can snail mail me by writing Michael Corrigan 1332433, Pack 1 Unit, 2400 Wallace Pack Rd, Navasota, TX 77868. Be sure to leave your return address. I can only receive email, not send them. Shout out to Phisher1.

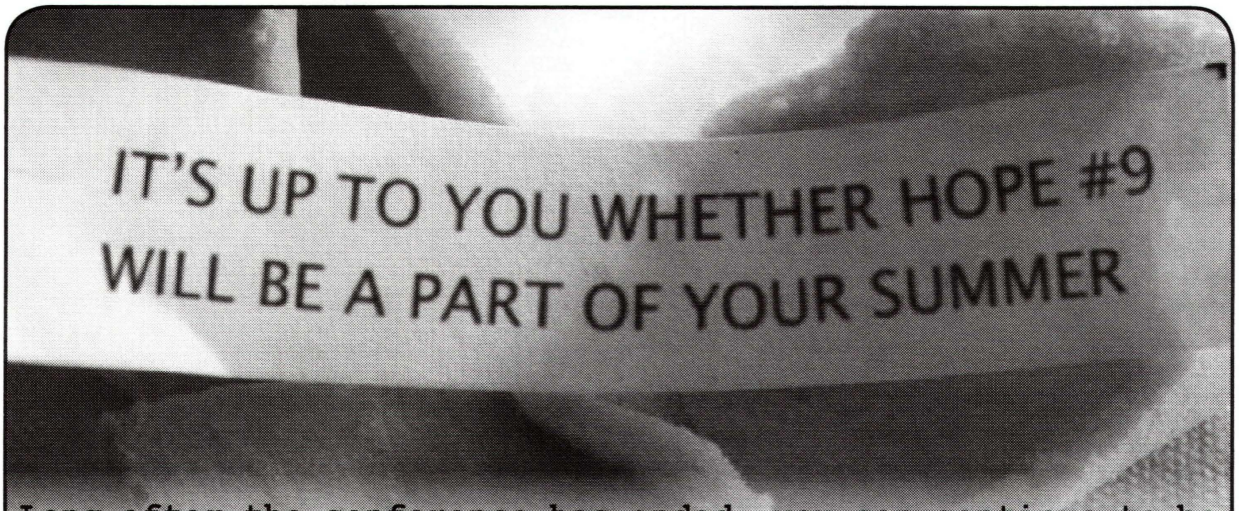
ISO PEN PALS, FRIENDS, CONTACTS. SWM 6' 170 BRN/BRN looking to network and exchange info with other users of master key system, remote viewing, cryptography, and law of attraction. I have resources in several offshore locations, looking for interested people to correspond with. 18+, race, sex, orientation not important. Bilingual English/Spanish, will answer all. Please write Jose Daniel Coryell, T-68127, CCI D5-44up, PO Box 608, Tehachapi, CA 93581.

LOOKING FOR PEN PALS. I'm Jesse McGraw (Ghost Exodus), an incarcerated hacker looking to connect with anybody willing to write. I'll respond to all letters. Originally from Oceanside CA/Dallas TX. I'm 28, 5 foot 8, 135 lbs, blue eyes, brown hair, tattoos. I'm into network security, 802.11 hacking, religion, paranormal, Linux, and music. www.myspace.com/blackfridaynull Write me @ Jesse McGraw #38690-177, PO Box 9000, Seagoville, TX 75159.

AT THE END OF THE HARDER THEY COME. 27 yrs male seeks correspondence. 6 foot, 200 lbs, black hair (buzzed), greenish eyes. Lots of tats, a few piercings. Interests include computers, networking, "remote networking," telco, wireless/radio tech+theory, history, politics, current events, revolutionary/national liberation movements/organizations, military history, Gaelic (Irish) language, urban exploration, tattoo art, music (electronic/house/"rave"/goth/industrial, punk/ska/hardcore, reggae, a bit of metal, some rap, some folk also). Incarcerated with about 2.5 to 3.5 years left, will respond to all. Can email if you post/snail mail your email address to me. Mike Kerr, 09496029, PO Box 9000-Low, Forrest City AR 72336.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

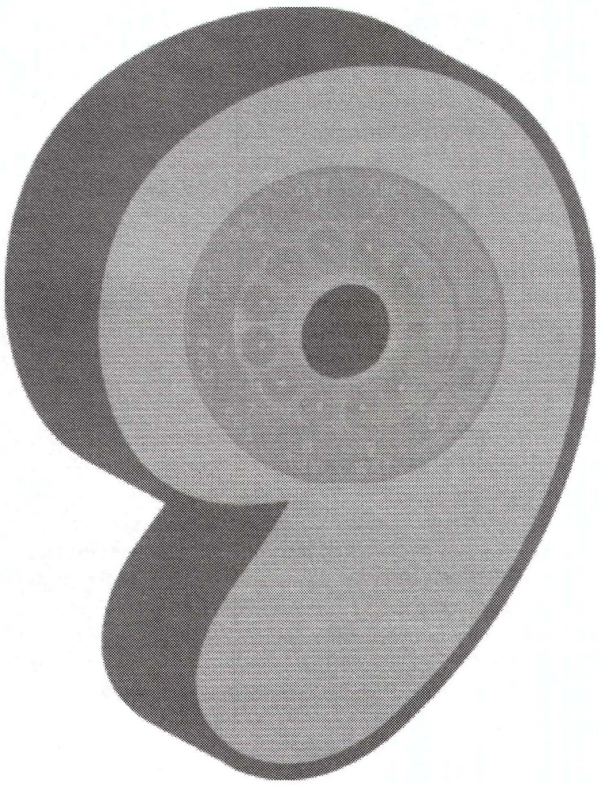
Deadline for Autumn issue: 8/21/12.



Long after the conference has ended, you can continue to be a part of it. Being present in person is, of course, the best thing in the world. But that doesn't last forever and, for some people, it doesn't happen at all. That's why we have our memories, which we are happy to transfer to others who never had them in the first place.

Look for well over 100 hours of video from HOPE Number Nine in DVD format, as well as various leftover relics, such as t-shirts and admission badges. We make the latter available for as long as possible, but they do run out, sometimes rather quickly. We make the DVDs available to preserve our history and share the joy of HOPE with those who can't make it.

We're also engaged in an ongoing project to digitize all of the older HOPE conferences, making them available both online and in higher quality DVD formats, without region coding or any kind of copy protection. What we need from you in order to make this project succeed is support. This type of thing takes time, money, and equipment to get it done right. The more people who buy our DVD sets, the easier it is for us to keep moving forward on this.



You can keep updated on all post-HOPE items at store.2600.com

"The Department of Justice does not endorse the organizations or views represented by this site and takes no responsibility for, and exercises no control over, the accuracy, accessibility, copyright or trademark compliance or legality of the material contained on this site." - Message on the Department of Justice website that appears when a visitor clicks on a link. This same agency routinely shuts down websites because of links they find objectionable.

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

S T A F F

Infrastructure
flyko

Network Operations
css, phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Forum Admins
Bunni3burn, dot.ret

Inspirational Music: Foster the People, Mosca, Slick Rick, Damien Marley, Yuksek, Masked Marauders, S.Mouse, Biz Markie, Awolnation, Shooter Jennings

Shout Outs: Crypt, Pan, Zap, Bob, Russell, Cyberjunkie, JA, Julia O'Dwyer, Cory Doctorow, Debra, SpaceX, Dave Mee, MadLab, Snocrash

Welcome: Mia

RIP: Sid

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 (ISSN 0749-3851, USPS # 003-176); Summer 2012, Volume 29 Issue 2, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2011 at $25 per year. (1987 only available in full back issue sets.) Individual issues available from 1988 on at $6.25 each. Subject to availability. Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2012; 2600 Enterprises Inc.

MEETINGS

ARGENTINA

Buenos Aires: Bar El Sitio, Av de Mayo 1354

AUSTRALIA

Melbourne: Softbelly Bar, 367 Little Bourke St, Melbourne. 6 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the wi-fi hotspot. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: Quick Restaurant, Place de la Republique. 6 pm

Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Newk's, 4925 University Dr.

Arizona

Phoenix: Citizen Expresso Bar, 4700 N Central Ave. 6 pm

Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Ft. Smith: Sweetbay Coffee, 7908 Rogers Ave. 6 pm

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Center (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Colorado Springs: The Enclave Coop, 2121 Academy Circle. 7 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Panera Bread, Fashion Square Mall.

Sebring: Lakeshore Mall food court, next to payphones. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm

Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Northampton: The Yellow Sofa, 24 Main St. 6 pm

Worcester: TESLA space - 97D Webster St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Las Vegas: Barnes & Noble Starbucks Coffee, 3860 Maryland Pkwy. 7 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Mexico

Albuquerque: Quelab Hacker/MakerSpace, 1112 2nd St NW. 6 pm

New York

Albany: Starbucks, 1244 Western Ave.

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College). 7 pm

North Dakota

Fargo: 222 E Market St, upstairs near the bar, but not in it. 6 pm

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.

Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

San Antonio: Bunsen Burger, 5456 Walzem Rd. 7 pm

Vermont

Burlington: Quarterstaff Gaming Lounge, 178 Main St, 3rd floor.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

More Global Payphones

Iceland. Found in Reykjavik on New Year's Eve, this is pretty much what you would expect a phone booth to look like up there at that time of year.

Photo by Eric H. Jung

India. Found in the streets of Mysore, this is one of the few remaining coin-operated phones. Naturally, it seems a bit worse for wear.

Photo by Howard Feldman

Ukraine. Seen in the city of Lviv, this is old-school in more ways than we can count.

Photo by Corey Sherman

Taiwan. A typical card reading phone spotted in Taipei.

Photo by Bruce Robin

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

This is really something you don't see very often. It comes from a semi truck tank with multiple compartments, a baffle system, and an overfill safety system. **Leighton Brooks** tells us that it fills until you release a valve (so that dead people can't operate it), and it runs 60 gallons or so over the amount it was released at. So this was quite a coincidence on a compartment that was already partially full.

Back in the day when everyone was red boxing at payphones, some of the devices were a lot larger than most. This one was so large that it had a bathroom attachment.
Found by **Bill Gaines** in Lake Grove, New York.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in!
Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription
(or back issues) or a *2600* t-shirt of your choice.